Studies on Some New Classes of Optical Orthogonal Codes

A Thesis Submitted

in Partial Fulfilment of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

by

MANOJ CHOUDHARY

to the

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

August, 2001

Certificate

It is certified that the work contained in the thesis entitled STUDIES ON SOME NEW CLASSES OF OPTICAL ORTHOGONAL CODES, by Manoj Choudhary, has been carried out under our supervision and that this work has not been submitted elsewhere for a degree.

(J. John)
Associate Professor
Department of Electrical Engineering
Indian Institute of Technology
Kanpur, INDIA

(P. K. Chatterjee)
Professor
Department of Electrical Engineering
Indian Institute of Technology
Kanpur, INDIA

August, 2001

Dedicated

To

My Parents

Acknowledgements

I wish to express deep sense of gratitude to my thesis supervisors, Dr. P. K. Chatterjee, and Dr. J. John, for their able guidance, advice, and continuous encouragement during the course of this work. Like true teachers, they understood my limitations. I am indebted to them for their patience during the difficult phases of this work.

It has been a great pleasure to learn and study in association with Dr. V. Sinha, Dr. P. R. K. Rao, Dr. M. C. Bhandari, Dr. Sumana Gupta, Dr. P. Sircar, Dr. S. K. Bose, Dr. A. K. Chaturvedi, Dr. K. S. Venkatesh, and Dr. M. U. Siddiqui. I am also thankful to Dr. P. Sinha of Department of Mathematics for his timely help.

I gratefully acknowledge my previous employer, ERNET Project at IIT Kanpur, for financial support during part of my stay here. I take this opportunity to thank my current employer, Novell Software Development (India) Ltd. Bangalore, for granting me adequate leave to bring the thesis to this stage of submission.

I had the privilege of having numerous friends who blessed my life. I pleasantly recall Srinidhi and Saroja, who despite being thousands of miles away from Kanpur, were never really too far. Hostel life, and the fun associated with it, would have been incomplete without friends like Atul, Vicky, Awasthi, Avi, Vishal, Suman, Kshitiz, Mishra, Shishir, Vineet, and Kodo. I will always cherish their affection.

Tomars (Satyendra and Shashi), Mudgils (Vivek, Nandini Bhabhi, Akshat and Avi), and Balvinders (Balvinder, Harpreet Bhabhi and Nayandeep) have treated me as a family member and provided great mental support.

My wife Bhawana has been a wonderful companion and has enriched my life with her presence. My limited vocabulary makes it difficult to describe her immense contribution.

Whatever little I have achieved in life, the credit goes to my family members: my sister Hemu, my brother Kishore, and my parents to whom I take great pride in dedicating this thesis. They have kept trust and faith in whatever I did.

Finally, a lot of thanks and gratitude to all those people whose names could not be mentioned here for the fear of running out of space.

Manoj Choudhary

Synopsis

The objective of the thesis is to design some new classes of Optical Orthogonal Codes. More specifically, we look at those classes of codes, which have smaller code lengths and better correlation properties. The codes discussed here are suitable for use in fiber optic code division multiple access (FO-CDMA) systems. Though our discussion has been centered around applications of these codes in the FO-CDMA systems, the codes can be used for any optical CDMA systems.

The rapid developments in optical signal processing and the advantages of fiber optic communications have provided the necessary impetus towards development of all optical networks. CDMA systems allow multiple users to simultaneously share a common channel asynchronously with little control amongst users, by assigning minimally interfering unique code sequences to different users. The vast bandwidth available in optical fiber channel makes it a natural medium for applications of CDMA, specially in fiber optic local area networks.

The need to have a large number of users in the FO-CDMA system requires a large number of minimally interfering code sequences assigned to different users. The optical systems (which combine the signals on power basis) require the codes to be orthogonal for truly (0,1) systems. Such codes have been referred to as Optical Orthogonal Codes (OOCs), and have many more 0's than 1's in them to approach orthogonality. An OOC, represented by $(n, w, \lambda_a, \lambda_c)$, has n as the length of each of its codewords, w is the number of 1's in each codeword (also called weight of the codeword), any codeword has a maximum off-peak autocorrelation of λ_a, and any two codewords in the OOC has a maximum value of crosscorrelation equal to λ_c. We denote the number of codewords in the OOC by M. Throughout the thesis, we have represented the codewords of the OOCs in the form of w-sets, where elements of the w-sets are integers modulo n and represent the locations of 1's in the code sequence.

Several classes of Optical Orthogonal Codes have been proposed in the last two decades. These include OOCs based on the Prime Sequences, Quadratic Congruences, Projective Geometry, and algebraic error correcting codes. In most of these codes, the length required to generate even a moderate number of codewords is quite large.

The study reported here is important for two reasons. First, the smaller length of codewords generated for a relatively large number of codewords allows higher data rates to be supported, for a given minimum laser pulse width. Secondly, the correlation values have been kept small which result in lower multiple user interference. Given the present trend of growth of optical networking, the requirement to have a large number of users in the system can only grow. We summarize some contributions of the thesis in the following.

Main Results

The thesis has been organized in seven chapters. In Chapter 1, we give an introduction of FO-CDMA systems and introduce the Optical Orthogonal Codes.

Chapter 2 contains a review of OOCs proposed earlier in the literature. We discuss the codes on the basis of their construction procedures and the code parameters. The OOCs discussed in this chapter include the Prime Sequence codes, the Quadratic Congruence codes, codes based on the Projective Geometry, two dimensional codes, 2^n Prime Sequence codes, and OOCs based on the error correcting codes. We include a few examples to illustrate the construction procedure and the characteristics of these codes. We briefly compare these existing codes on the basis of their parameters.

In Chapter 3, we propose a new class of OOCs based on the well known Hadamard matrices. First, we generate the difference sets by a truncation of the Hadamard matrices. These difference sets are then converted to w-sets, with each w-set representing a codeword. We illustrate the construction procedure with the help of suitable examples, and show the parameters of the OOCs constructed using this method.

Later, we present a generalized construction procedure for generation of the codewords for this class of OOCs. The OOCs constructed using this approach are of the form $(4t-1, 2t-1, t-1, t)$, where t is a positive integer. This class of OOCs, can be constructed for any length $n = 4t-1$, if a Hadamard matrix exists for an order $(n+1)$.

Chapter 4 is concerned with the development of another new class of Optical Orthogonal Codes using the Skolem Sequences. The basic idea in this chapter is to put integers in the w-sets in such a way that the off-peak autocorrelation and crosscorrelation constraints are satisfied. A translated version of Skolem sequences is proposed to put distinct integers as the distances between 1's in a w-set, for a code of weight $w = 3$.

The correlation constraints never exceed a value of 1 for this class of codes, as all the distances between 1's are distinct. We explain the generation of codewords with the help of a few examples. This class of codes gives us codewords having minimum lengths for a given number of codewords. This class of OOCs has M codewords, each of which has a length of $6M+1$, weight 3 and the correlation parameters $\lambda_a = \lambda_c = 1$. The requirement for generation of codewords for this class of OOCs is that the number of codewords, M, should be congruent to either 0 (modulo 4) or 1 (modulo 4).

We present methods to construct three more new classes of OOCs in Chapter 5. Each class has a different set of code parameters. First, we suggest a method to generate codewords of an Optical Orthogonal Code using the Table of Primes. These are variants of the Prime Sequence codes and give us codewords with better off-peak autocorrelation value λ_a, while trading off the crosscorrelation constraint. These codes are of the form $(p^2 - p, p - 1, 1, p - 2)$, where p is a prime number.

Next, we suggest a method to construct OOCs by partitioning the Galois Field $GF(n)$, where n is a prime number of the type $n = 3t + 2$. The constraint here is that 3 must be a primitive root of n. The $GF(n)$ is partitioned into t number of 3-sets. We illustrate the construction procedure using an example. The off-peak autocorrelation and crosscorrelation values of the resultant codewords never exceed a value of 2. The codes are of the form $(3t + 2, 3, 2, 2)$, and the number of codewords is t.

The OOCs based on the Quadratic Residues are then proposed as the third method. These codes are constructed using the quadratic residues of a prime number and the construction procedure is explained using an example. This code can be constructed for any prime number and the resultant codewords have the maximum off-peak autocorrelation and crosscorrelation values of 2. The code suggested here is better than the OOCs based on the Quadratic Congruences, since the maximum crosscorrelation value is reduced from 4 to 2, while keeping all other parameters the same. These codes have the form $(p^2, p, 2, 2)$, where p is a prime number.

A comparison of the codes proposed in this thesis with the codes suggested earlier is presented in Chapter 6. We make this comparison on the basis of number of codewords generated for the given code parameters, and their ability to tolerate multiple access interference. We discuss the superiority of the OOCs proposed in this thesis and their relevance to Fiber Optic CDMA systems. We observe that the OOCs constructed using a prime number as their basis, such as, Prime Sequences, Quadratic Congruences, Quadratic Residues, etc., are not optimal from the point of view of the number of codewords generated for given code parameters against the Johnson bound.

In Chapter 7, we summarize important conclusions of the thesis and give suggestions for future work.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Code division multiple access (CDMA) is a spread spectrum communication technique in which several users simultaneously share a common channel by assigning different minimally interfering code sequences to different user pairs. In CDMA, users communicate data by multiplying their message bits with their own assigned unique codes. A matched filter at the receiver detects the data by correlating the received sequence with its assigned code sequence. This approach sufficiently reduces multiple access interference with the help of correlation detection.

The requirement of a very large bandwidth limits the use of CDMA in systems where the bandwidth is not at a premium.

Optical fiber is such a medium where virtually unlimited bandwidth is available, and high capacity systems can be implemented using the CDMA technique. However, a substantial propagation delay compared to transmission time makes CDMA more suitable to Fiber Optic local area networks (LANs). The fact that CDMA supports asynchronous transmissions, is particularly helpful when the transmissions are asynchronous, random and bursty as in the case of LANs.

The rapid developments in optical signal processing [1] and the advantages of fiber optic communications are leading towards all optical networks [2]. The use of CDMA in fiber optic LANs has been proposed by Salehi et. al. in [3–6]. An experimental system for fiber optic CDMA (FO-CDMA) is given in [7–9].

1.1 Fiber Optic CDMA

One way of achieving CDMA in optical fiber networks is by first spreading the information signal from the data source using electrical means and then converting it into optical form to be launched in the optical fiber. In systems using electrical-to-optical and optical-to-electrical conversions, because of the limited speed of electronic signal processors, the maximum data transmission rate is severely limited. Furthermore, the signal processing speed becomes more critical than the communication speed in the design of optical fiber communication systems, since the electrical processes are much slower than the optical processes.

Another way of achieving optical CDMA by first converting the signal into optical form and then spreading it in the optical domain itself is, therefore, a much better alternative. Efforts have been made to develop optical components to perform signal processing functions optically. Signal processing operations are possible using single mode optical fibers because of their excellent propagation and delay properties [10]. For very high bandwidth (in excess of 100 GHz) applications, the optical fiber delay line signal processors have been studied instead of charge coupled devices (operating frequency less than 10 MHz), surface acoustic wave devices (operating frequency of the order of several hundred MHz), and magnetostatic wave devices (operating frequency ranges from 2 - 12 GHz).

Apart from FO-CDMA systems, optical CDMA systems such as Spatial Optical CDMA [11], Holographic CDMA [12], Coherent Optical CDMA [13, 14], Coherent ultrashort light pulse CDMA [15, 16], Optical frequency hop multiple access system [17, 18], and Optical CDMA using spectral encoding of sources [19–21] have also been proposed. The problem of multimedia transmission in fiber optic networks using

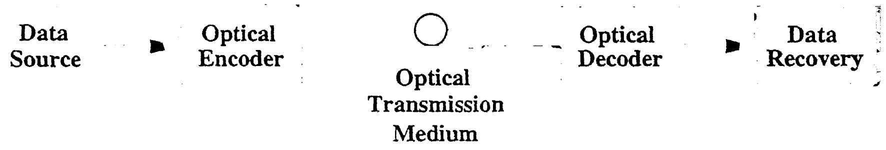

Figure 1.1.1: A typical link in a FO-CDMA system

CDMA has been addressed in [22,23].

The fiber optic CDMA takes advantage of excess bandwidth in single mode fibers to map low information rate electrical or optical signals into high rate optical pulse sequences to achieve random access communications, with little network control among the users. The term chip rate is the rate of the spreading optical pulse sequence, and chip duration is the pulse duration of this optical sequence. A typical link in a FO-CDMA communication system is shown in Fig. 1.1.1.

The optical encoder maps each message bit of output information into a very high rate optical sequence, that is then coupled into a single mode fiber. At the receiver end, the optical pulse sequence is correlated with a stored replica of itself and the sampled output at the end of the bit interval is then compared with a predetermined thresold level for data recovery. A FO-CDMA system having M such users (transmitter-receiver pairs) in a STAR configuration is shown in Fig. 1.1.2.

The most common structure used for optical encoding and decoding is based on optical delay lines [10,24] and is shown in Fig. 1.1.3. The lengths of the delay lines are adjusted such that a pulse of one chip duration at the input is mapped to the chip positions having a value of "1" of the specified code sequence. The number of delay lines is equal to w, where w is the number of 1's in the codeword (known as code weight) used in the FO-CDMA system. Then lengths of the delay lines in the decoder are such that a 1 delayed by j chips in the encoder is delayed by $(n-j)$ chips

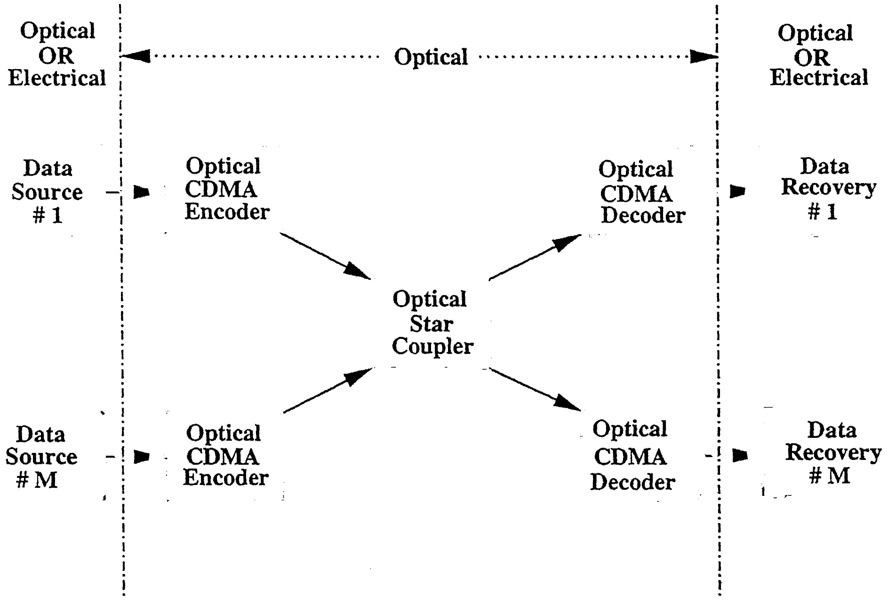

Figure 1.1.2: A FO-CDMA system in star configuration with M users

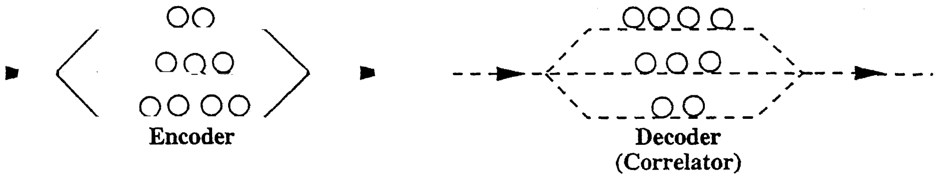

Figure 1.1.3: A Delay line structure for optical encoder and decoder

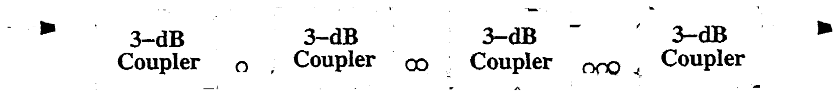

Figure 1.1.4: A Lattice structure for optical encoder(decoder)

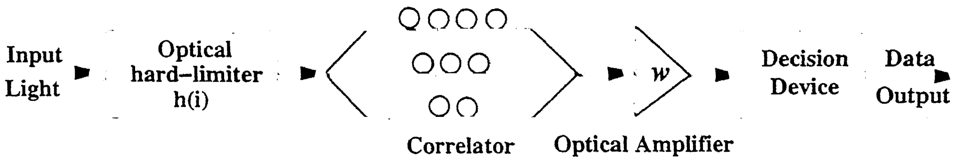

Figure 1.1.5: A receiver involving hard-limiter and optical amplifier

in the decoder, where n is the length of its code sequence. The number of delay lines required in the decoder is also equal to w.

However, there is a power loss due to splitting and combining into the delay lines. This power loss is proportional to w each at both the encoder and the decoder. For larger w, the power losses are quite significant. In order to compensate the losses, optical amplifiers may be used both in the encoder and the decoder, as shown in Fig. 1.1.5. The gain of the optical amplifier at each end is kept equal to w.

Another approach to encoding and decoding is through lattices and ladder networks [25–29]. These ladder networks are made of cascaded 3-dB (2 x 2) couplers. An m-stage network consists of $(m+1)$ fixed 3-dB couplers connected in cascade. In these networks, the power loss due to encoding and decoding is only 3-dB at each end. However, the weight of the codewords must be equal to 2^m, where an m-stage ladder network is used. Fig. 1.1.4 shows such a serial structure for encoding and decoding.

A hard-limiter is used to limit the interference patterns to be a (0,1) form, which might otherwise have been multilevel due to superposition of signals from several users [30]. The characteristics of the optical hard-limiter is given by

$$h(i) = \begin{cases} 1 & \text{for } i \geq 1 \\ 0 & \text{for } i < 1 \end{cases}$$

where i is the input light intensity at the limiter input. A hard-limiter is shown in Fig. 1.1.5.

In order to extract data from the desired optical pulse sequence at the receiver in the presence of all other users' pulse sequences, we need to design code sequences that satisfy two conditions [4], namely:

1) each sequence should be easily distinguishable from a shifted version of itself, and

2) each sequence should be easily distinguishable from (a possibly shifted version of) every other sequence in the set.

The above two conditions imply that the autocorrrelation of any code sequence (except for zero shift) should be small, and the maximum crosscorrelation between any two code sequences should be zero. However, (0,1) sequences for truly positive systems, such as optical systems, can not achieve a crosscorrelation value of 0, as the coincidences do not cancel out unlike in (-1,+1) sequences. Hence, the minimum possible value of crosscorrelation is 1. Such codes are referred to as Optical Orthogonal Codes[1].

1.2 Optical Orthogonal Codes

In this section, we introduce various parameters and notations used in the Optical Orthogonal Codes (OOCs).

An $(n, w, \lambda_a, \lambda_c)$ Optical Orthogonal Code C is a family of (0,1) sequences of length n and weight w that satisfy the following bound on maximum off-peak autocorrelation λ_a:

$$\sum_{t=0}^{n-1} x_t x_{t+\tau} \leq \lambda_a, \tag{1.2.1}$$

for any code sequence (also referred as codeword) $X = \{x_0, x_1, \ldots, x_{n-1}\} \in C$ and any integer shift τ such that, $0 < \tau < n$. The maximum crosscorrelation λ_c satisfy

[1] Since maximum crosscorrelations cannot be 0 in case of (0,1) codes, optical codes with small values of crosscorrelation are referred to as Optical Orthogonal Codes (OOCs) in the literature

the following bound:

$$\sum_{t=0}^{n-1} x_t y_{t+\tau} \leq \lambda_c, \tag{1.2.2}$$

for any two code sequences X, Y such that $X \neq Y \in C$ and any integer shift τ such that, $0 \leq \tau < n$.

Since each code sequence of C has a Hamming weight w, therefore, the autocorrelation peak for any code sequence is w. This happens for zero delay (i.e., $\tau = 0$). A codeword of length n has chip positions from 0 to $(n-1)$.

An $(n, w, \lambda_a, \lambda_c)$ Optical Orthogonal Code C can also be considered as a family of w-sets of integers modulo n, in which each w-set corresponds to a codeword, and the integers within each w-set specify the nonzero bit positions of the codeword. Then the correlation properties can be reformulated as given below:

1) the autocorrelation property:

$$|(a+X) \cap (b+X)| \leq \lambda_a, \tag{1.2.3}$$

for any $X \in C$ and any $a \not\equiv b \pmod{n}$, and

2) the crosscorrelation property:

$$|(a+X) \cap (b+Y)| \leq \lambda_c, \tag{1.2.4}$$

for any $X \neq Y \in C$ and any a, b.

Here $a + X = \{a + x : x \in X\}$ and all integers under consideration are taken modulo n. The set theoretic notion offers a convenient notation for OOCs when w is much smaller than n. In the set theoretic perspective, autocorrelation and the crosscorrelation properties can also be interpreted as follows:

1) autocorrelation: for any $X \in C$, any integer $c \neq 0$ can be represented as the difference $x - x'$, with $x, x' \in X$, in at most λ_a ways, and

2) crosscorrelation: for every pair of w-sets $X \neq Y \in C$, any integer $c \neq 0$ can be represented as the difference $x - y$, with $x \in X$, $y \in Y$, in at most λ_c ways.

The size of a code C, denoted by M, is the number of codewords in it. The cyclic shift of a codeword is not considered as another codeword. The largest possible size of an $(n, w, \lambda_a, \lambda_c)$ code is denoted by $\Phi(n, w, \lambda_a, \lambda_c)$. A code that has the maximum possible size, $M = \Phi(n, w, \lambda_a, \lambda_c)$, is said to be an optimal code. The Johnson bound for $\Phi(n, w, \lambda_a, \lambda_c)$ is given in [31,32] as,

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{(n-1)(n-2)\ldots(n-\lambda)}{w(w-1)(w-2)\ldots(w-\lambda)} \right\rfloor, \qquad (1.2.5)$$

where $\lambda = max(\lambda_a, \lambda_c)$ and $\lfloor x \rfloor$ means largest integer less than or equal to x.

The maximum number of simultaneous users in the system, K, affects the signal-to-noise ratio (SNR) at the receiver[2]. The SNR is given by the ratio of the square of the peak of the autocorrelation value to the variance of the amplitude of the interference. When K users are transmitting simultaneously, the total interference at the desired receiver is the superposition of the $(K-1)$ different crosscorrelations. If the $(K-1)$ interferers are uncorrelated, then the variance of the total interference is equal to the sum of the variances of the $(K-1)$ crosscorrelations. In general, the calculation of average variance is a lengthy process, particularly if we take larger code lengths.

In a FO-CDMA system, a "0" corresponds to no light and a "1" corresponds to maximum light intensity. As the optical systems are positive systems, an error occurs only if the desired receiver wrongly decides a "1" instead of a transmitted "0". However, when a "1" is transmitted, there will be no error because it cannot be converted to a "0"in any case.

For error-free transmission, assuming multiple access interference to be the only source of noise present, autocorrelation peak w should ideally be larger than $(K-1)\lambda_c$, where K is the number of simultaneous users in the system. We should choose the thresold level "T" equal to the autocorrelation peak w in order to reduce the

[2] Here we assume multiple access interference to be the only source of noise.

probability of bit error. When the threshold is less than or equal to the maximum value of the multiple access interference, i.e., when $w \leq (K-1)\lambda_c$, then the errors due to interfering signals occur with finite probability. This represents the worst case scenario. Some upper bounds on the multiple access interference have been obtained by finding expressions for the probability density functions of the interferers using optical disk patterns for $(n, w, 1, 1)$ codes [4,5].

It is desirable to have OOCs with the largest possible number of codewords M, given the parameters n, w, λ_a and λ_c. A good optical orthogonal code has many more 0's than 1's in each code sequence as that reduces the number of coincidences. Optical codes approach orthogonality (achieve quasi-orthogonality) by minimizing coincidences rather than by cancellation.

1.3 Motivation for the Work

In the orthogonal sequences for (-1,1) systems such as Walsh-Hadamard sequences [33], the orthogonality is achieved by having an equal number of 1's and -1's in the code sequences so that the crosscorrelations become zero. Though Gold codes were suggested earlier for use in optical CDMA systems [34], but they required encoding and decoding in the electrical domain, thus not using the vast bandwidth available in the optical domain. The positivity of the optical systems require (0,1) sequences to be designed with a fundamental difference, that there is no way of cancelling the values of coincidences. This means that the minimum value of λ_c is equal to 1, and the only way to approach orthogonality is by designing sequences that have a small number of 1's in them compared to 0's.

The requirement to have a small number of 1's in the code sequences to obtain orthogonal sequences and the desire to have a large number of such orthogonal codes (which correspond to the number of users in the FO-CDMA system), makes the code lengths comparatively longer. However, the length of the codewords can not be increased indefinitely as that limits the maximum data rates that can be supported. The longer length will require either laser pulse width to be smaller, or the supported data rate to go down. There are practical constraints on the minimum value of the laser pulse width, so the maximum data rates are limited.

Various OOCs, such as those based on the Prime Sequences, Quadratic Congruences, Projective Geometry, Error correcting codes etc., have been proposed earlier in the literature. All these codes, except those based on the Projective Geometry, have very large code lengths compared to the number of codewords obtained. Even to have a moderate number of users in the FO-CDMA systems (or equivalently, to have a moderate number of codewords in the OOC), the code length becomes prohibitively large. One approach to shortening the code length is suggested by Argon et. al. [35]. This method involves finding the location of the last 1 in all the codewords, and considering that as the length of the codewords, i.e., all subsequent zeroes are removed. However, this results in a violation of correlation constraints.

Another important factor, that needs to be simultaneously taken care of, is the maximum value of off-peak autocorrelation and crosscorrelation. These values have to be kept small, as the maximum number of simultaneous users in the system is limited by the multiple access interference.

We have attempted to design several new classes of Optical Orthogonal Codes towards meeting these objectives of having a large number of codewords for smaller code lengths, and for lower values of maximum correlation parameters. These factors make the proposed OOCs relevant to the FO-CDMA systems.

Throughout the thesis, we have used the set theoretic notation to describe the codewords. This notation is useful when we have a smaller number of 1's than 0's, which is the case in Optical Orthogonal Codes. Our emphasis in this work has been on the construction of new classes of codes rather than the implementation of encoder and decoder.

1.4 Contributions and Organization of the Thesis

This thesis is concerned with developing a few classes of Optical Orthogonal Codes that have a large number of codewords for a given length. The maximum off-peak autocorrelation and maximum crosscorrelation values for the codewords are kept small. The codewords are represented in set theoretic notation. In this section, we discuss the contributions of the thesis and its organization.

A critical review of the Optical Orthogonal Codes, proposed earlier in the literature, is presented in Chapter 2. We discuss the codes on the basis of their construction procedures and the code parameters. The OOCs discussed in this chapter include the Prime Sequence codes, the Quadratic Congruence codes, codes based on the Projective Geometry, two dimensional codes, 2^n Prime sequence codes and OOCs based on the error correcting codes. A few examples have been included for illustrating the construction procedure and the characteristics of these codes. We briefly compare these existing codes on the basis of their parameters.

In Chapter 3, we propose a new class of OOCs based on the well known Hadamard matrices. Here we follow the approach of generating the difference sets by a truncation of the Hadamard matrices. These difference sets are then converted to w-sets, with each w-set representing a codeword. We illustrate the construction procedure with the help of suitable examples, and show the parameters of the codes constructed using this method. Later, we present a generalized construction procedure for the generation of the codewords for this class of OOCs. The codewords, for this class of OOCs, can be constructed for any length n, if a corresponding Hadamard matrix exists for an order $(n + 1)$.

Chapter 4 is concerned with the development of another new class of Optical Orthogonal Codes using the Skolem Sequences. The basic idea in this chapter is to put the integers in the w-sets in such a way that the off-peak autocorrelation and crosscorrelation constraints are satisfied. A translated version of the Skolem sequences is suggested for putting distinct integers in a w-set, for $w = 3$, such that the correlation constraints never exceed a value of 1. We explain the generation of codewords with the help of a few examples. This class of codes gives us codewords of smaller lengths for a given number of codewords.

In Chapter 5 of the thesis, we present methods to construct three more new classes of OOCs, each having a different set of code parameters. First, we suggest a method to generate the codewords of an Optical Orthogonal Code using the Table of Primes. These codes are variants of the Prime Sequence codes and give us codewords with better off-peak autocorrelation value λ_a, while trading off the crosscorrelation constraint.

Next, we suggest a method to construct OOCs by partitioning the Galois Field $GF(n)$, where n is a prime number of the type $n = 3t + 2$. The constraint here is that 3 must be a primitive root of n. The $GF(n)$ is partitioned into t number of 3-sets. We illustrate the construction procedure using an example. The off-peak autocorrelation and crosscorrelation values of the resultant codewords never exceed a value of 2.

The Optical Orthogonal Codes based on the Quadratic Residues are then proposed in the third method. These codes are constructed using the quadratic residues of a prime number and the construction procedure is explained using an example. This code can be constructed for any prime number and the resultant codewords have the maximum off-peak autocorrelation and crosscorrelation values of 2. The class of OOCs suggested here is better than the OOCs based on the Quadratic Congruences, since the maximum crosscorrelation value is reduced from 4 to 2, while keeping all other parameters the same.

A comparison of the proposed codes in this thesis with the codes suggested earlier in the literature is presented in Chapter 6. We make this comparison on the basis of the ability of codewords to tolerate multiple access interference and the number of codewords available for the given code parameters. We discuss the superiority of the OOCs proposed in this thesis and relevance to Fiber Optic CDMA systems.

Chapter 7 concludes the thesis. The suggestions for future work are also included in this chapter.

The thesis includes four appendices: Appendix A contains a brief exposure to Difference families, Appendix B contains existence conjectures for Hadamard matrices, Appendix C presents existence and construction of Skolem sequences, and in Appendix D, a Table of Primes and their primitive roots is given.

Chapter 2

A Review of Optical Orthogonal Codes

The $(n, w, \lambda_a, \lambda_c)$ Optical Orthogonal Code is a family of (0,1) sequences of length n and weight w that satisfies the bounds on λ_a and λ_c, as discussed in the previous chapter. The earliest OOC, reported in the literature, was constructed using Prime Sequences by Shaar et. al. [36]. The codewords of this class of OOCs are generated using time-mapped elements of Galois Field $GF(p)$ for a prime number p. Chung et. al. [32] presented several construction techniques of OOCs using combinatorics and projective geometry. They also presented iterative constructions of OOCs. Holmes et. al. [37] introduced "Quasi-Prime" codes that possess the symmetry structure required for generation by lattice structures [26].

In order to have a large number of codewords in an OOC, we require larger lengths of codewords, which puts practical constraints on the minimum laser pulse width available to support high data rates. To overcome this, Park et. al. [38] proposed encoding in two dimensions such as Temporal/Spatial codes.

To mitigate the problem of high value of off-peak autocorrelation of Prime Sequence codes, Marić [39] introduced OOCs based on Quadratic Congruences. Another class of OOCs, called 2^n codes, was proposed by Kwong et. al. [40,41], to reduce high power losses in the implementation of OOCs by optical delay lines [10,24]. These 2^n

codes use serial lattice architectures for their generation.

In this chapter, we review various classes of OOCs that have been proposed earlier in the literature and briefly compare them on the basis of various code parameters. A few variants of the above classes of OOCs have also been proposed in the literature. We cite their references when we discuss these classes of OOCs.

2.1 OOCs based on Prime Sequences

In this section, we discuss the construction of the OOCs based on Prime Sequences [36].

Construction: Consider a Galois Field of order p, $GF(p)$, where p is a prime number. Using $GF(p) = \{0, 1, 2, \ldots, p-1\}$, we construct a prime sequence S_x^p , where

$$S_x^p = \{s_x^p\ (0),s_x^p\ (1),\ldots,s_x^p\ (p-1)\}\ ,$$

by multiplying every element j of $GF(p)$ by an element x of $GF(p)$ modulo p, i.e.,

$$s_x^p(j) = x.j \quad (\text{mod p}) \quad \text{for } x, j \in GF(p). \tag{2.1.1}$$

Thus we can obtain p distinct prime sequences. Each of these prime sequences is then mapped into a binary code sequence C_x^p , where

$$C_x^p = \{c_x^p\ (0),c_x^p\ (1),\ldots,c_x^p\ (n-1)\}\ ,$$

using the following rule:

$$c_x^p(i) = \begin{cases} 1 & \text{for } i = s_x^p(j) + jp\ \ (mod\ \ p);\ \ j = 0, 1, \ldots, p-1 \\ 0 & \text{otherwise} \end{cases} \tag{2.1.2}$$

In this way, we can construct an optical code with length $n = p^2$ and weight $w = p$. The number of such codewords is p.

Example 2.1.1: OOC USING PRIME SEQUENCES FOR $p = 5$

For p=5, we have n = 25.

$S_0^5 = \{0\ \ 0\ \ 0\ \ 0\ \ 0\}$

$S_1^5 = \{0\ \ 1\ \ 2\ \ 3\ \ 4\}$

$S_2^5 = \{0\ \ 2\ \ 4\ \ 1\ \ 3\}$

$S_3^5 = \{0\ \ 3\ \ 1\ \ 4\ \ 2\}$

$S_4^5 = \{0\ \ 4\ \ 3\ \ 2\ \ 1\}$

The corresponding codewords are as follows:

$C_0^5 = \{10000\ \ 10000\ \ 10000\ \ 10000\ \ 10000\}$

$C_1^5 = \{10000\ \ 01000\ \ 00100\ \ 00010\ \ 00001\}$

$C_2^5 = \{10000\ \ 00100\ \ 00001\ \ 01000\ \ 00010\}$

$C_3^5 = \{10000\ \ 00010\ \ 01000\ \ 00001\ \ 00100\}$

$C_4^5 = \{10000\ \ 00001\ \ 00010\ \ 00100\ \ 01000\}$

The autocorrelation of codeword C_0^5 and C_3^5 of example 2.1.1 is shown in Fig. 2.1.1 and Fig. 2.1.2, respectively. As can be seen from Figs. 2.1.1 and 2.1.2, the peak value of autocorrelation is equal to the weight of the code (which is 5 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) does not exceed 4 in the plots. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_2^5 and C_4^5 for example 2.1.1 is shown in Fig. 2.1.3. As can be seen from Fig. 2.1.3, the maximum crosscorrelation value between the two codewords never exceeds 2.

As seen above, C_x^p is divided into p frames, each frame containing p chips. The code C_x^p is therefore a time-mapped, binary version of the sequence S_x^p .

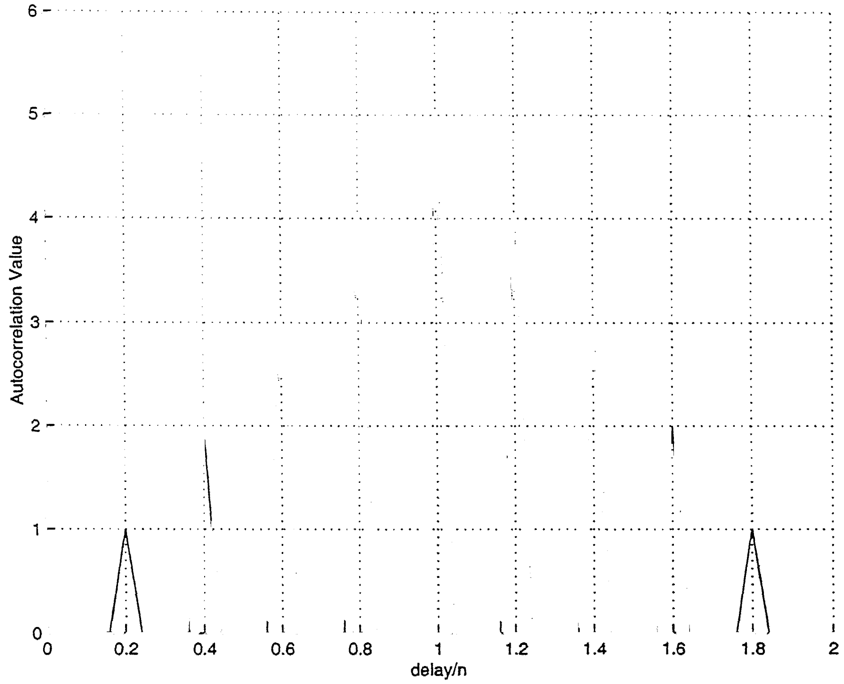

Figure 2.1.1: Autocorrelation of codeword C_0^5 of a (25,5,4,2) OOC based on Prime Sequences

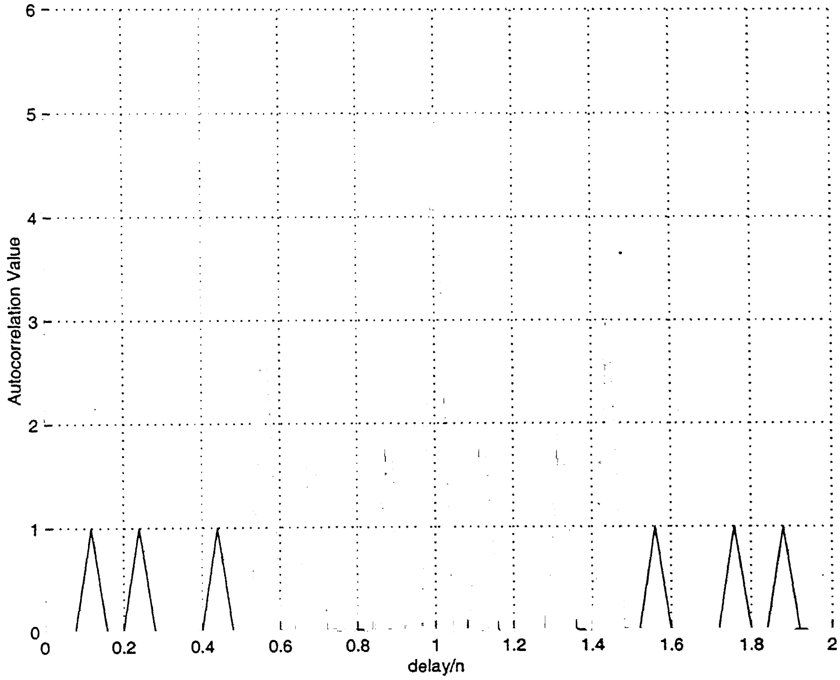

Figure 2.1.2: Autocorrelation of codeword C_3^5 of a (25,5,4,2) OOC based on Prime Sequences

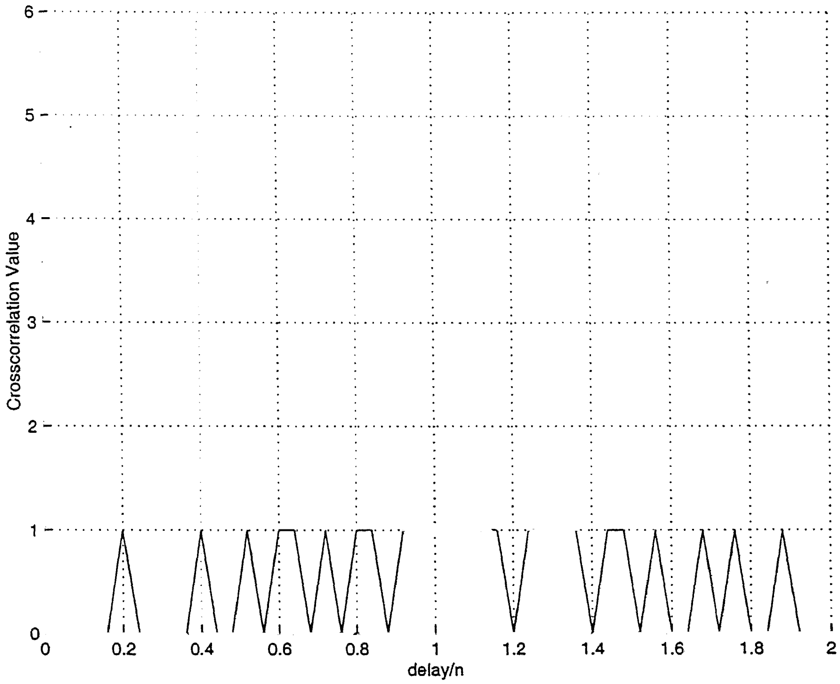

Figure 2.1.3: Crosscorrelation between codeword C_2^5 and C_4^5 of a (25,5,4,2) OOC based on Prime Sequences

2.1.1 Properties of OOCs using Prime Sequences

The codewords generated using the Prime sequences have the following properties:

- The length of the codewords, $n = p^2$
- The weight of the codewords, $w = p$
- The maximum value of off-peak autocorrelation, $\lambda_a = p - 1$
- The maximum value of crosscorrelation, $\lambda_c = 2$
- The number of codewords, $M = p$

Pruncal et. al. [42] gave an experimental demonstration of an Optical CDMA LAN using Prime Sequences codes. Later on Pruncal et. al. [43] extended the experiments to suggest the use of Prime Sequence codes in an Optical Synchronous CDMA system.

The performance of the Prime Sequence codes in optical CDMA systems has been analysed in [44,45].

2.2 "Quasi-Prime" Optical Orthogonal Codes

Optical codes are generated and decoded using optical delay lines [10,24], as shown in section 1.1. Other methods used to generate the optical codes are by employing fiber optic lattices [25,26].

Fiber optic lattices are used to generate optical codes having symmetrical location of 1's from either end. Prime Sequence codes, since they do not satisfy the necessary symmetry requirements, are not amenable to generation by fiber optic lattices. The symmetry property is useful because the lattices can act as their own matched filters (a property that requires time-reversibility of impulse responses).

"Quasi-prime" codes [37] are extended (or contracted) and time-shifted versions of Prime Sequence codes that satisfy the symmetry property, and hence, can be generated using fiber optic lattices.

Construction: From a Prime Sequence code C_x^p as defined in section 2.1, we obtain the "Quasi-Prime" code C_{xk}^{rp} of length rp chips as

$$c_{xk}^{rp}(i) = c_x^p([i+kp]_n) \quad where \;\; i = 0, 1, \ldots, (rp-1). \tag{2.2.1}$$

Thus a "Quasi-Prime" code C_{xk}^{rp} is a time shifted and extented (or contracted) version of the Prime Sequence code C_x^p . C_{xk}^{rp} has r number of one's.

Example 2.2.1: "QUASI-PRIME" OOC FOR $p = 5$

For p= 5, and $n = 25$, we have from Example 2.1.1,

$C_2^5 = \{10000 \;\; 00100 \;\; 00001 \;\; 01000 \;\; 00010\}$

$C_4^5 = \{10000 \;\; 00001 \;\; 00010 \;\; 00100 \;\; 01000\}$

Choosing $r = 4$ and $k = 4$, we obtain

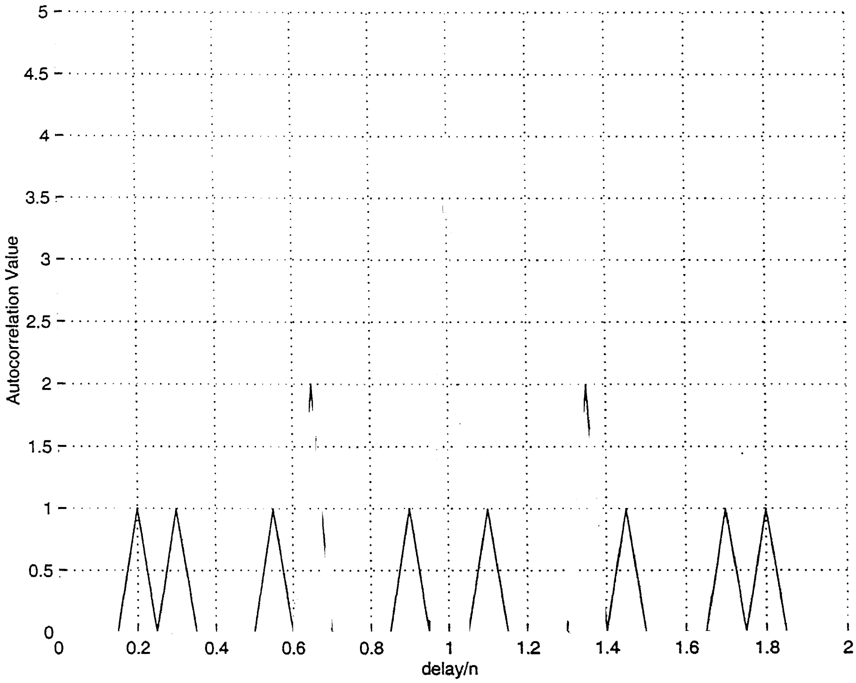

Figure 2.2.1: Autocorrelation of codeword C_{24}^{45} of a (20,4,3,2) OOC based on "Quasi-Prime" Sequences

$C_{24}^{45} = \{00010\ \ 10000\quad 00100\ \ 00001\}$

$C_{44}^{45} = \{01000\ \ 10000\quad 00001\ \ 00010\}$

Similarly for $r = 8$ and $k = 2$, we have

$C_{42}^{85} = \{00010\ \ 00100\ \ 01000\ \ 10000\quad 00001\ \ 00010\ \ 00100\ \ 01000\}$

The autocorrelation of codeword C_{24}^{45} and C_{44}^{45} of example 2.2.1 is shown in Fig. 2.2.1 and Fig. 2.2.2, respectively. As can be seen from Figs. 2.2.1 and 2.2.2, the peak value of autocorrelation is equal to the weight of the code (which is $r = 4$ in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) does not exceed 3 in the plots. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_{24}^{45} and C_{44}^{45} of example 2.2.1 is shown in Fig. 2.2.3. As can be seen from Fig. 2.2.3, the maximum crosscorrelation value between the two codewords never exceeds 2.

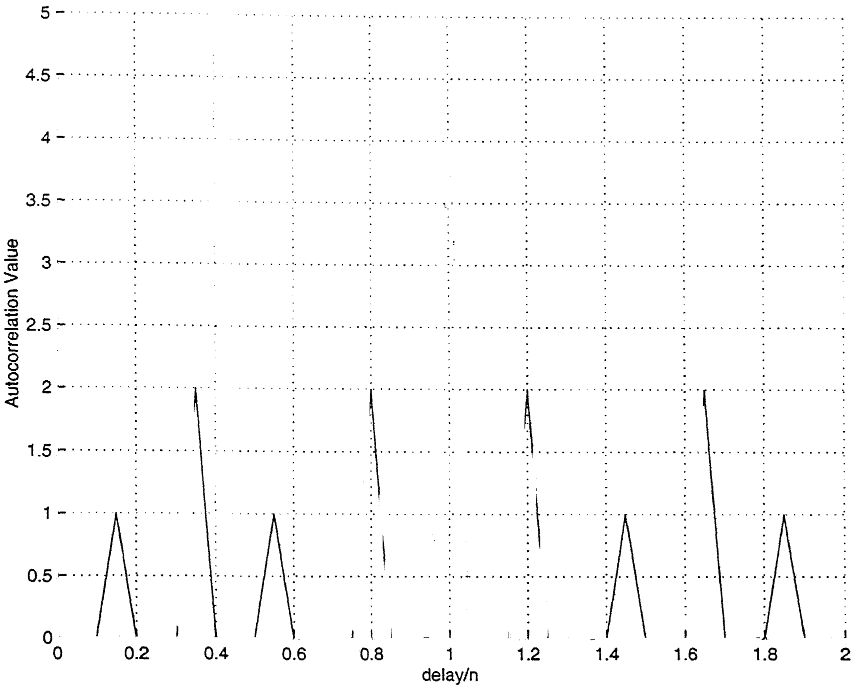

Figure 2.2.2: Autocorrelation of codeword C_{44}^{45} of a (20,4,3,2) OOC based on "Quasi-Prime" Sequences

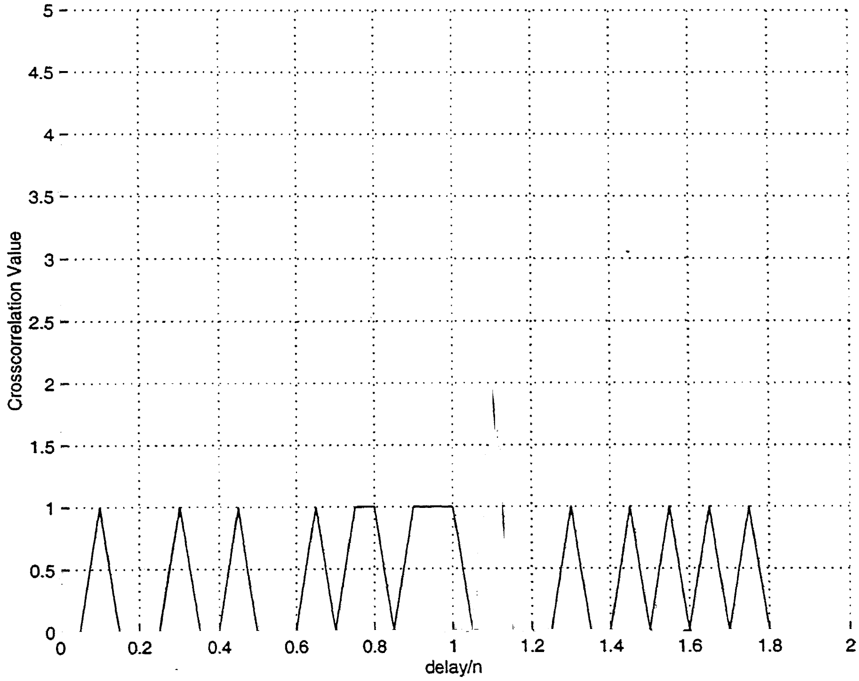

Figure 2.2.3: Crosscorrelation between codewords C_{44}^{45} and C_{24}^{45} of a $(20, 4, 3, 2)$ OOC based on "Quasi-Prime" Sequences

All the codewords of an Optical Orthogonal Code need to be of same length, therefore, different "Quasi-Prime" codes having different lengths (such as C_{44}^{45} and C_{42}^{85}), derived from the same Prime Sequence code (C_4^5), can not act as distinct orthogonal members of a codeword set. Therefore, the "Quasi-Prime" code C_{xk}^{rp} has the same number p of maximum codewords as the Prime Sequence code C_x^p . The number r is generally chosen to be the nearest power of two to a given number p, which itself is chosen to correspond to the maximum number of distinct codes required in the codeword set.

2.2.1 Properties of "Quasi-Prime" OOCs

The codewords of "Quasi-Prime" OOCs have the following properties:

- The length of the codewords, $n = rp$, $(\Lambda - 1)p < r < \Lambda p$, r and Λ are integers.
- The weight of the codewords, $w = r$
- The maximum value of off-peak autocorrelation, $\lambda_a = (p-1)\Lambda$
- The maximum value of crosscorrelation, $\lambda_c = 2\Lambda$
- The number of codewords, $M = p$

2.3 OOCs based on Quadratic Congruences

In this section, we discuss the construction of OOCs based on Quadratic Congruences. We review some basic parameters of quadratic congruences first.

1) The quadratic congruence is defined as

$$y(k+1) \equiv [y(k) + (k+1)] \ \ (mod \ \ p),$$

where $y(0) = 0,\ \ 0 \leq k \leq p-1$, p is a prime.

2) Quadratic placement operator $y_x(k)$ is expressed by the relation:

$$y_x(k) \equiv \frac{xk(k+1)}{2} \quad (mod\ \ p),$$

where $0 \leq k \leq p-1,\ \ 0 < x \leq p-1$.

The quadratic placement operator $y_x(k)$ is also represented in the form of an array for the sake of convenience.

3) The placement difference function, which represents the difference between two quadratic placement operators for any given shift, is given by

$$(y_\beta(k)\Delta y_\alpha(k))_{a,b} = y_\beta(k+a) - y_\alpha(k) - b,$$

where $|a|, |b| \leq p-1$. Here variables a and b denote integer horizontal and vertical shifts, respectively.

Construction: An Optical Orthogonal Code using Quadratic Congruences can be constructed in the following manner [39]:

For each user x, the code sequence C_x^p , where

$$C_x^p = \{c_x^p\ (0), c_x^p\ (1), \ldots, c_x^p\ (n-1)\},$$

and

$$c_x^p(i) = \begin{cases} 1 & \text{if } y_x(k) + kp = i\ \ (mod\ \ p);\ \ x = \{1, \ldots, p-1\} \text{ and } k = \lfloor \frac{i}{p} \rfloor \\ 0 & \text{elsewhere} \end{cases} \tag{2.3.1}$$

where p is a prime and $y_x(k)$ is the quadratic placement operator.

Example 2.3.1: OOC USING QUADRATIC CONGRUENCES

Let us take $p = 5$ and $x = 2$. We have the four quadratic placement operators as

$y_1^k = \{0 \;\; 1 \;\; 3 \;\; 1 \;\; 0\}$

$y_2^k = \{0 \;\; 2 \;\; 1 \;\; 2 \;\; 0\}$

$y_3^k = \{0 \;\; 3 \;\; 4 \;\; 3 \;\; 0\}$

$y_4^k = \{0 \;\; 4 \;\; 2 \;\; 4 \;\; 0\}$

The corresponding codewords are:

$C_1^5 = \{10000 \;\; 01000 \;\; 00010 \;\; 01000 \, 10000\}$

$C_2^5 = \{10000 \;\; 00100 \;\; 01000 \;\; 00100 \, 10000\}$

$C_3^5 = \{10000 \;\; 00010 \;\; 00001 \;\; 00010 \, 10000\}$

$C_4^5 = \{10000 \;\; 00001 \;\; 00100 \;\; 00001 \, 10000\}$

Thus there are p 1's in the sequence of length $n = p^2$. The number of codewords is equal to $(p - 1)$.

The autocorrelation of codeword C_3^5 of example 2.3.1 is shown in Fig. 2.3.1. As can be seen from Fig. 2.3.1, the peak value of the autocorrelation is equal to the weight of the code (which is 5 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) does not exceed 2 in the plot.

The crosscorrelation between codewords C_4^5 and C_1^5 of example 2.3.1 is shown in Fig. 2.3.2. As can be seen from Fig. 2.3.2, the maximum crosscorrelation value between the two codewords never exceeds 4.

2.3.1 Properties of OOCs using Quadratic Congruences

The codewords generated using the Quadratic Congruences have the following properties:

- The length of the codewords, $n = p^2$
- The weight of the codewords, $w = p$

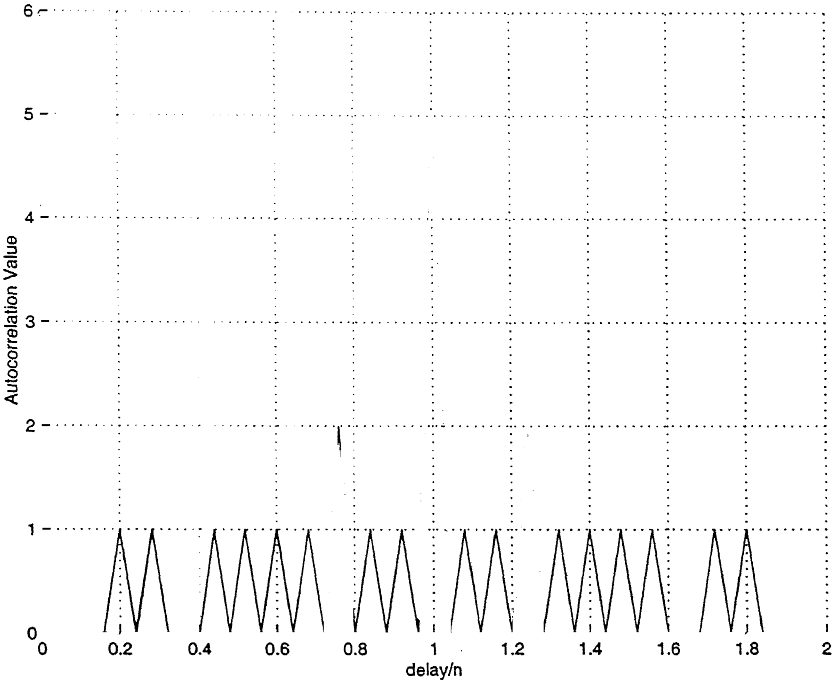

Figure 2.3.1: Autocorrelation of codeword C_3^5 of a (25,5,2,4) OOC based on Quadratic Congruences

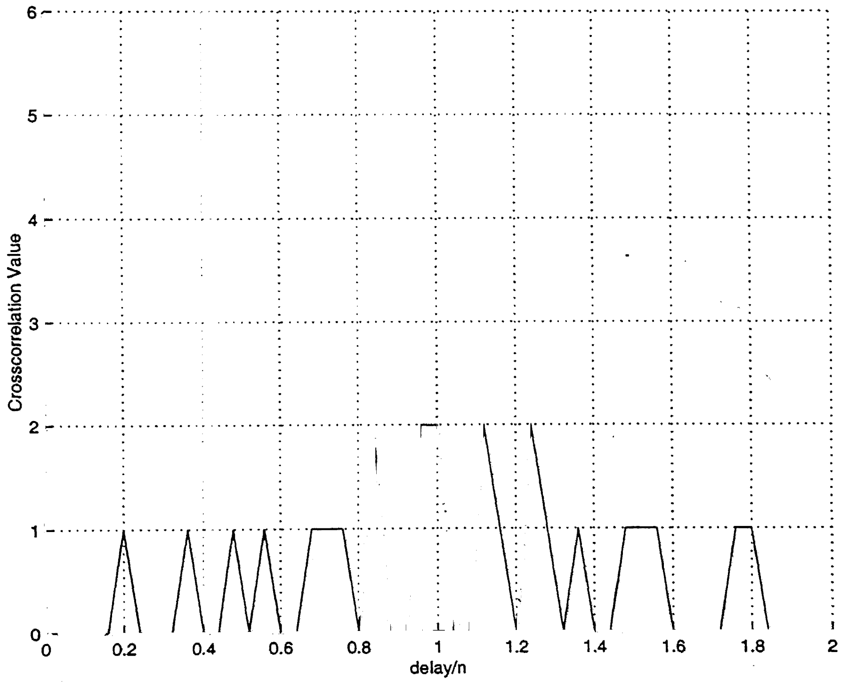

Figure 2.3.2: Crosscorrelation between codeword C_4^5 and C_1^5 of a (25,5,2,4) OOC based on Quadratic Congruences

- The maximum value of off-peak autocorrelation, $\lambda_a = 2$
- The maximum value of crosscorrelation, $\lambda_c = 4$
- The number of codewords, $M = p - 1$

Marić [46] presented a variant of Quadratic Congruence (QC) code, called Extended Quadratic Congruence (EQC) code, where he extended the length of the codeword to reduce the values of λ_a and λ_c. The resultant codewords form the $(p(2p-1), p, 1, 2)$ EQC code.

In general, synchronous access schemes produce higher throughput than asynchronous techniques, when users with regular traffic patterns are transmitting [47]. An analysis of Quadratic Congruence codes, for synchronous case, is done in [48].

2.4 Projective Geometry based OOCs

In this section, we discuss the construction and properties of Optical Orthogonal Codes using Projective Geometry [32,49]. We later generalize these codes and give a set of codewords using generalized procedure [32,50].

The most important example of projective geometry $PG(m, q)$ of order m is that obtained from $GF(q)$. Some important facts regarding $PG(m, q)$ are summarised here for ready reference.

1) Number of points in $PG(m, q)$, $n = \frac{q^{m+1}-1}{q-1}$.

2) Number of points on a line, $w = q + 1$.

3) $PG(m, q)$ with $m = -1$ is an empty set, $m = 0$ is a point, and $m = 1$ is a line.

4) $PG(m, q)$ is constructed from a vector space $V(m + 1, q)$ of dimension $(m + 1)$ over $GF(q)$ by taking one-dimensional subspaces of V to be the points of $PG(m, q)$ and the two-dimensional subspaces of V to be lines.

5) Total number of lines, $M_1 = \binom{n}{2} / \binom{w}{2}$.

6) As a corollary of (4), there are $\frac{q^{m+1}-1}{q-1}$ distinct lines through the origin in $V(m+1, q)$. Points in projective geometry correspond to lines through the origin in $V(m+1, q)$.

Construction: An Optical Orthogonal Code using Projective Geometry approach can be constructed in the manner described below [32].

In a finite projective geometry $PG(m, q)$, any two lines intersect at no more than one point. We use lines in $PG(m, q)$ as codewords in the Optical Orthogonal Codes. First we describe the method for constructing an OOC with $\lambda_a = \lambda_c = \lambda = 1$. Two codewords (represented by lines in $PG(m, q)$) thus intersect at no more than one point, as desired. Since the cyclic shift of a codeword is a codeword, therefore, the cyclic shift of a line should also be a line. However, in order to find values of autocorrelation and crosscorrelation of these codewords, we need to implement cyclic shifts of lines maintaining the same number of points on the shifted line. The positions of points now change on the shifted line.

A vector β in the vector space $V(m+1, q)$ has $(m+1)$ coordinates with values from finite field $GF(q)$ or alternatively it can be regarded as an element β of the extension field $GF(q^{m+1})$. If α is the primitive element of $GF(q^{m+1})$, then there are $(q^{m+1}-1)$ nonzero elements ranging from 0^{th} to $(q^{m+1}-2)^{th}$ powers of α . If $\alpha^i = \beta$, where i is any integer between 0 and $(q^{m+1}-2)$, then the discrete logarithm $\log_\alpha \beta = i$. Therefore, the discrete logarithm establishes a one-to-one correspondence between nonzero vectors in $V(m+1, q)$ and the integers $(0, 1, \ldots, q^{m+1}-2)$. Since a vector in $V(m+1, q)$ is a point in $PG(m, q)$, hence log(.) is a one-to-one mapping between points of $PG(m, q)$ and the integers modulo n. Since each line in $PG(m, q)$ is a collection of points, therefore each line is also a subset of integers modulo n with each point corresponding to an integer modulo n. Furthermore, let the cyclic shift of

Table 2.4.1: Elements of $GF(2^3)$

power of primitive element	The binary equivalent
α^0	001
α^1	010
α^2	100
α^3	101
α^4	111
α^5	011
α^6	110

a line L in $PG(m,q)$ correspond to a set of points $\{p : \log p = (1 + \log p') \pmod{n}\}$ for every point p' on L. Then the cyclic shift of a line is still a line in $PG(m,q)$.

Definition 2.4.1 An orbit is a set of lines in $PG(m,q)$ that are cyclic shifts of each other. The number of lines in a orbit is called its size, which is a divisor of n. An orbit is full if its size is n, otherwise it is incomplete. The number of codewords is equal to the number of full orbits in the set.

Example 2.4.1: OOC USING PROJECTIVE GEOMETRY

Let us take $PG(m,q)$ with $m = 2$ and $q = 2$. Therefore, the number of points, $n = \frac{q^{m+1}-1}{q-1} = 7$, the number of points on a line, $w = q+1 = 3$, and the number of lines $M_1 = \frac{n(n-1)}{w(w-1)} = 7$. Using $GF(q^{m+1})$, i.e., $GF(2^3)$ and taking $X^3 + X^2 + 1$ as the primitive polynomial, we have Table 2.4.1.

The lines of $PG(2,2)$ are shown in Table 2.4.2. Now the cyclic shift of any line, say d, by any shift, say 5, is equal to

$$d + 5 \Rightarrow (1,2,6) + 5 \pmod{7} = (6,0,4) \Rightarrow c.$$

Thus we see that cyclic shift of every line is another line here. The number of orbits is equal to $\frac{M_1}{n} = 1$, which is full, containing all seven lines. Picking any representative line, we have a $(7,3,1,1)$ OOC with only one codeword.

Table 2.4.2: Lines of $PG(2,2)$

Name of line	The constituent points (integers modulo n)
a	(0,1,5)
b	(0,2,3)
c	(0,4,6)
d	(1,2,6)
e	(1,3,4)
f	(2,4,5)
g	(3,5,6)

2.4.1 Generalized Construction of Projective Geometry based OOCs

The OOCs generated using Projective Geometry require larger lengths of codewords for a moderate number of codewords, if $\lambda = 1$. Here we present a generalized construction procedure for OOCs based on Projective Geometry [32, 50] which allows us to generate codewords with $\lambda \geq 1$. By relaxing the value of λ, we can obtain a large number of codewords for relatively smaller code lengths. In order to have codewords defined for higher values of $\lambda_a = \lambda_c = \lambda$, we use the notion of s-spaces. The s-space with $s = 1$ indicates a line. An s-space in a $PG(m, q)$ corresponds to $(s+1)$-dimensional space through the origin in $V(m+1, q)$. Once we define the s-spaces for the code, the rest of the construction procedure is similar to the one described earlier.

Here we describe the properties of generalized $PG(m, q)$ codes:

1) Number of points in $PG(m, q)$, $n = \frac{q^{m+1}-1}{q-1}$.

2) Number of points in the s-space, $w = \frac{q^{s+1}-1}{q-1}$.

3) The intersection of two s-spaces is atmost an $(s-1)$-space. Therefore λ is equal to the number of points in the $(s-1)$-space. Its value is given by $\lambda = \frac{q^s-1}{q-1}$.

4) The cyclic shift of an s-space is also an s-space. The orbit is the set of all

s-spaces that are cyclic shifts of each other. The size of an orbit necessarily divides n. The number of codewords is equal to the number of complete orbits.

5) A codeword consists of discrete logarithm of points in each representative s-space.

6) Total number of s-spaces, $M_s = \binom{n}{s+1} / \binom{w}{s+1}$.

7) Total number of codewords constructed using $PG(m,q)$ for a given value of s is equal to $M = \lfloor \frac{M_s}{n} \rfloor$.

8) The code constructed using $PG(m,q)$ with a given value of s is optimal if and only if $\lfloor \frac{M_s}{n} \rfloor = \frac{M_s}{n}$.

Example 2.4.1.1: OOC USING PROJECTIVE GEOMETRY

We take $PG(4,2)$ with $s = 2$. The parameters of the generated codewords are:

1) Number of points, $n = \frac{2^{4+1}-1}{2-1} = 31$.

2) Number of points in the s-space, $w = \frac{2^{2+1}-1}{2-1} = 7$.

3) $\lambda = \frac{2^2-1}{2-1} = 3$.

4) Total number of s-spaces, $M_2 = \lfloor \binom{31}{2+1} / \binom{7}{2+1} \rfloor = 128$.

5) The number of codewords constructed, $M = \lfloor \frac{M_2}{31} \rfloor = 4$.

The generated codewords are:

$C_1 = (0,1,2,8,10,12,22)$

$C_2 = (0,1,2,19,21,23,28)$

$C_3 = (0,1,2,6,7,11,24)$, and

$C_4 = (0,1,3,6,8,15,17)$

The code constructed using $PG(4,2)$ is not optimal because $\lfloor \frac{M_2}{31} \rfloor \neq \frac{M_2}{31}$ for $s = 2$. The s-spaces in the incomplete orbit are $(0,1,2,3,4,5,9)$, $(0,1,2,13,14,15,25)$, $(0,1,2,16,17,18,20)$ and $(0,1,2,26,27,29,30)$.

The autocorrelation of codeword C_1 and C_3 of example 2.4.1.1 is shown in Fig.

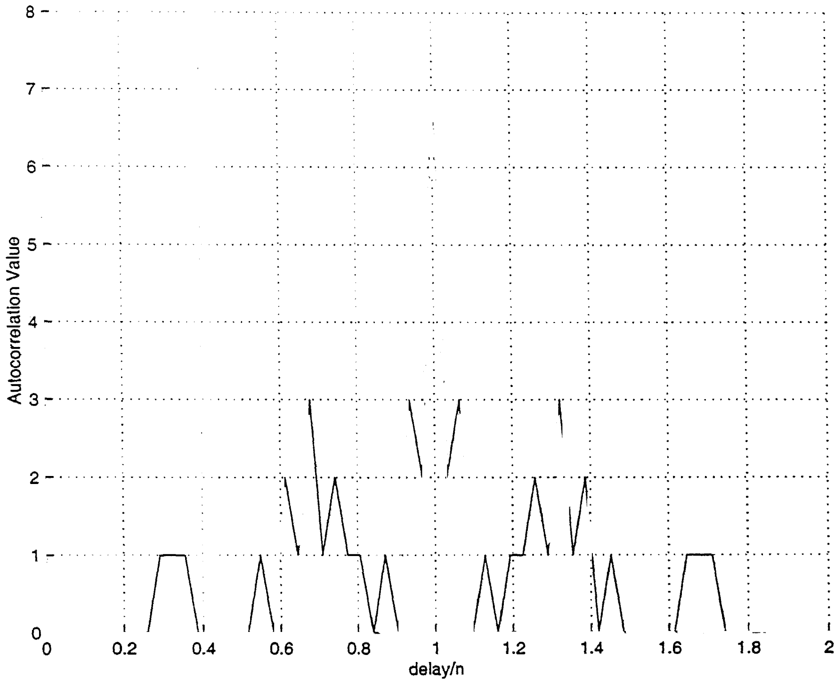

Figure 2.4.1: Autocorrelation of codeword C_1 of a (31,7,3,3) OOC based on Projective Geometry

2.4.1. and Fig. 2.4.2, respectively. As can be seen from Figs. 2.4.1 and 2.4.2, the peak value of autocorrelation is equal to the weight of the code (which is 7 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) does not exceed 3 in the plots. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_2 and C_3 of example 2.4.1.1 is shown in Fig. 2.4.3. As can be seen from Fig. 2.4.3, the maximum crosscorrelation value between the two codewords never exceeds 3.

2.5 Temporal/Spatial Codes

In this section, we review two-dimensional Optical Orthogonal Codes. The length of codewords increases dramatically as the number of codewords required increases. Increased length of the codewords significantly limits the data rates that can be

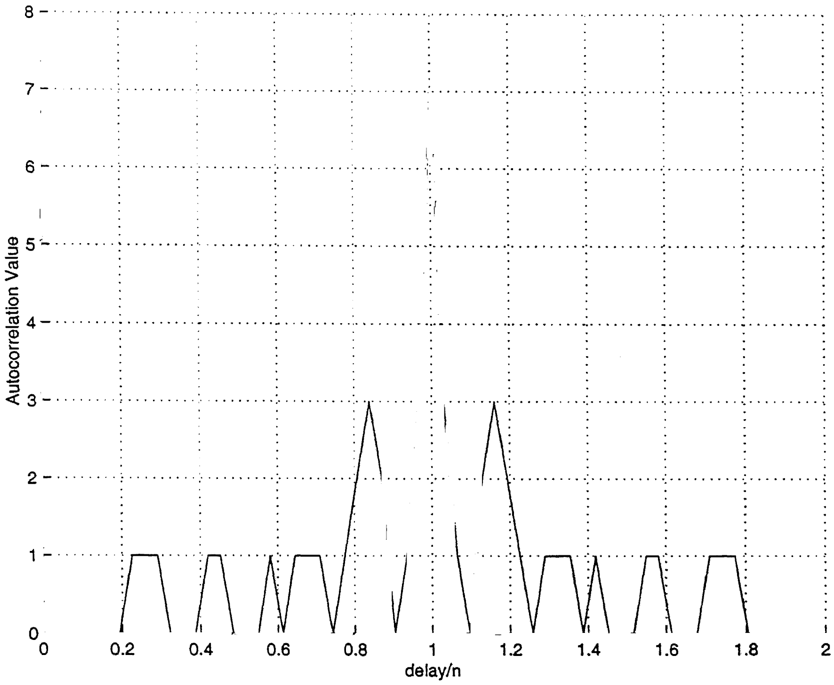

Figure 2.4.2: Autocorrelation of codeword C_3 of a (31,7,3,3) OOC based on Projective Geometry

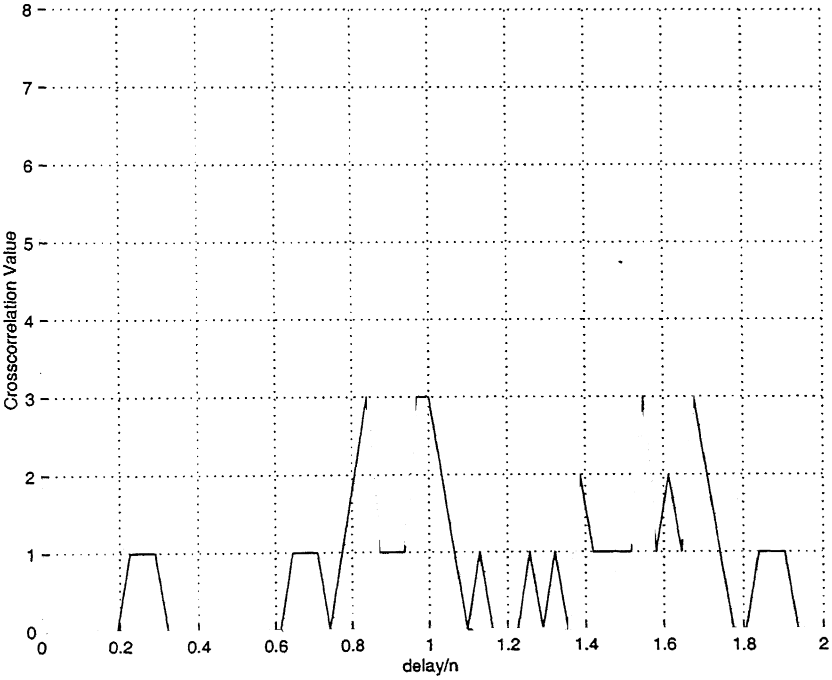

Figure 2.4.3: Crosscorrelation between codeword C_2 and C_3 of a (31,7,3,3) OOC based on Projective Geometry

supported. The increased length reduces the chip time and so we need lasers with smaller pulse widths to generate the codewords for a given data rate. The practical constraints on the minimum possible laser pulse width, and the requirement to support higher data rates, necessitate that the lengths of codewords should not increase indefinitely even when we want to maximize the number of users.

Towards this objective, Park et. al. proposed coding in two dimensions such as Temporal/Spatial (T/S) Codes [38]. The resultant codes are written in the form of a matrix, with rows and columns representing the two dimensions. Each row is an independent temporal code, and different rows are transmitted through different spatial channels. They demonstrated a T/S Single Pulse per Row (SPR) code based fiber optic CDMA network.

A Temporal/Spatial code is represented as $TS(n, w, R, P, \lambda_a, \lambda_c)$ of temporal length n, weight w, number of rows (spatial channels) R, number of pulses per row P, maximum off-peak autocorrelation λ_a, and maximum crosscorrelation λ_c. The total number of codewords is M.

Shivaleela et. al. gave a construction technique [51, 52] for T/S codes for Single Pulse per Row ($P = 1$) and $\lambda_c = 1$. A single pulse per row implies a maximum off-peak autocorrelation value of 0, as there is only a single 1 in every row.

The construction is for any $R \leq M$ codes with the above properties. Each row has a length $n = p$, where p is the smallest prime number such that $p \geq M$. The number p is a group under addition modulo p with elements $(0, 1, \ldots, p-1)$.

Given M, choose a prime number $p \geq M$. A T/S code C_i, $0 \leq i \leq R-1$, is generated by one of the elements j of the group p using the following three equations [51]:

$$R_0(j) = j \quad \text{for } j = 0, 1, \ldots, p-1 \tag{2.5.1}$$

$$R_i(j) = R_{i-1}(j) + j \pmod{p} \tag{2.5.2}$$

where,

$$C_i = \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ R_{p-1} \end{bmatrix} \tag{2.5.3}$$

The set of all the C_i form the T/S code. Each C_i is the canonical form representation of the two dimensional SPR codes. The T/S Code C can be written as

$$C = \begin{bmatrix} C_0 & C_1 & \ldots & C_{p-1} \end{bmatrix} \tag{2.5.4}$$

2.5.1 T/S codes using Prime Sequences

We suggest an alternative approach for construction of T/S codes using the Prime sequences discussed in section 2.1. This approach is simpler than that given in [51]. The construction is for any $R \leq M$ codes with $P = 1$, $\lambda_c = 1$, and $\lambda_a = 0$. Each row has a length $n = p$, where p is the smallest prime number such that $p \geq M$.

Given M, choose a prime number $p \geq M$. A T/S code C is generated by writing the corresponding Prime sequences S_x^p, for all $x = 0, 1, \ldots, p-1$, rowwise. The Prime sequences S_x^p are as defined in section 2.1. Thus $C_x = [S_x^p]$, where $1 \leq x \leq p$. The code is given as

$$C = \begin{bmatrix} S_0^p \\ S_1^p \\ \vdots \\ S_x^p \\ S_{p-1}^p \end{bmatrix} \tag{2.5.5}$$

Some other approaches towards construction of two dimensional codes and their properties are given in [53–55]. An experimental demonstration of two dimensional encoding is given in [56]. Three dimensional codes using Space/Wavelength/Time as the three dimensions has been suggested by Kim et. al. [57].

2.6 2^n Prime Sequence Codes

In this section, we briefly discuss 2^n Prime Sequence codes proposed by Kwong et. al. [40, 41]. The aim was to have a structure of encoder and decoder such that power losses could be reduced. Towards this, they suggested a serial coding architecture for the generation of OOCs. The encoder in the serial architecture consists of a tunable optical delay line with $M + 1$ stages of 2 x 2 couplers and optical delays. Here $M = \lceil log_2 w \rceil$, where w is a prime number. Here $\lceil x \rceil$ means smallest integer greater than or equal to x.

By assigning a differential delay of $2^{M-m}\tau$ to the m^{th} stage, any discrete time delay of $\{0, \tau, 2\tau, \ldots, (w-1)\tau\}$ can be generated, where $m = \{1, 2, \ldots, M\}$ and τ is the chip width. The decoder can be realised by a serial combination of 2 x 2 couplers, with suitable differential delays in each stage. The lesser number of optical couplers results in substantial cost reduction.

The 2^n Prime Sequence codes are variants of the Prime Sequence codes [36] such that the weight of every codeword is of the form 2^n. The 2^n codes are defined as a collection of binary N-tuples with weight of 2^n. In the serial structure, the distribution of present 2^m pulses is very restrictive, and strongly depends upon the previous 2^{m-1} pulses, where $1 < m \leq n$.

We include here a brief description of the construction procedure [40, 41]. The pulse distribution constraints can be more conveniently expressed in terms of "delay distribution" constraints [40]. The construction procedure for generating a 2^n Prime Sequence code involves forming the prime sequences, S_i, of weight $w > 2^n$, as given in section 2.1, and determining whether the delay distribution constraint is satisfied for each prime sequence.

If the constraint is satisfied, then the prime sequence is modified as follows: (i) the elements $s_{i,j}$ and $s_{i,j+1}$, whose delay satisfy the constraints, are kept unchanged while the remaining elements are replaced by X's, (ii) we discard an S_i if none of the delays satisfies the constraints, and (iii) the codewords of 2^n Prime Sequence codes are formed by time-mapping each modified prime sequence S_i into a binary code sequence. Every X in the modified prime sequence is mapped to p zeroes, where p is the prime number used to generate the prime sequences.

We have replaced $(w - 2^n)$ 1's of the prime sequences by 0's in the 2^n Prime Sequence codes, to satisfy the delay distribution constraints, therefore, the off-peak autocorrelation value λ_a and the maximum crosscorrelation value λ_c are never worse than those of the Prime Sequence codes. The number of codewords is less than that of Prime Sequence code of the same length.

Block multiplexing codes using ladder networks for incoherent all-optical systems have been presented by Tančevski et. al. [58].

2.7 OOCs using Error Correcting Codes

In this section, we discuss the construction of Optical Orthogonal Codes using constant weight error correcting codes. A t error correcting code is represented by (n, d), where n is the length of the codewords, and d is the minimum distance between any two codewords such that $d \geq 2t + 1$ [31]. When the weight w of all the codewords in the code is same, the resultant code is referred to as constant weight error correcting code (n, d, w).

The Optical Orthogonal Codes are equivalent to constant weight error correcting codes [32,59] with a minimum distance of $(2w-2\lambda)$, since two OOCs with parameters $(n, w, \lambda_a, \lambda_c)$ intersect at no more than λ places, where $\lambda = max(\lambda_a, \lambda_c)$. Therefore, to construct an $(n, w, \lambda_a, \lambda_c)$ OOC, we must examine $(n, 2w - 2\lambda, w)$ constant weight error correcting code and choose only those codewords whose cyclic shifts are also codewords. A table of constant weight codes is given in [60]. Some constructions for constant weight codes are given in [61–63].

We have included here four examples using the approach described above.

Example 2.7.1: OOC USING (19,4,3) ERROR CORRECTING CODES

From (19,4,3) constant weight error correcting code, we get OOCs with $n = 19$, $w = 3$, and $\lambda = 1$.

The resultant codewords are:

$C_1 = (12, 17, 18)$

$C_2 = (11, 15, 18)$, and

$C_3 = (8, 16, 18)$

Example 2.7.2: OOC USING (25,4,3) ERROR CORRECTING CODES

From (25,4,3) constant weight error correcting code, we get OOCs with $n = 25$, $w = 3$, and $\lambda = 1$.

The resultant codewords are:

$C_1 = (21, 22, 24)$

$C_2 = (13, 18, 24)$

$C_3 = (11, 15, 24)$, and

$C_4 = (10, 16, 24)$

As the length of the codewords is increased in this example, compared to example 2.7.1, the number of codewords is larger since we have an increased possibility of placing 1's.

Example 2.7.3: OOC USING (18,4,4) ERROR CORRECTING CODES

From (18,4,4) constant weight error correcting code, we get OOCs with $n = 18$, $w = 4$, and $\lambda = 2$.

The resultant codewords are:

$C_1 = (13, 15, 16, 17)$

$C_2 = (11, 12, 16, 17)$

$C_3 = (10, 11, 13, 17)$

$C_4 = (9, 12, 14, 17)$

$C_5 = (8, 9, 16, 17)$

$C_6 = (7, 13, 14, 17)$

$C_7 = (7, 11, 15, 17)$

$C_8 = (6, 10, 15, 17)$

$C_9 = (6, 8, 14, 17)$

$C_{10} = (5, 10, 14, 17)$, and

$C_{11} = (5, 7, 12, 17)$

Example 2.7.4: OOC USING (19,6,5) ERROR CORRECTING CODES

From (19,6,5) constant weight error correcting code, we get OOCs with $n = 19$, $w = 5$, and $\lambda = 2$.

The resultant codewords are:

$C_1 = (11, 13, 16, 17, 18)$

$C_2 = (6, 8, 10, 17, 18)$

$C_3 = (4, 9, 15, 17, 18)$, and

$C_4 = (3, 8, 12, 15, 18)$

In this example, we considered an increase in the length of the codewords by adding an extra 1, compared to example 2.7.3. Therefore, we have $n = 19$, and $w = 5$. Since, we still want $\lambda = 2$, the number of codewords is reduced as the number of possibilities of placing 1's is reduced.

2.8 Other Methods of Constructing OOCs

In this section, we briefly mention some other methods proposed for constructing OOCs. The construction procedures for these codes are not included.

Optical Orthogonal Codes are related to the theory of block design [32]. A t-(n, b, r, w, λ) design consists of n objects and b blocks of these objects. Each object is contained in r blocks, each block containing w objects. Each pair of t-objects is contained in exactly λ blocks. However, the intersection of two blocks is not small in general. Due to the balanced structure of the design, some block designs have good intersection properties. We can select a collection of blocks from a design and test if the autocorrelation and crosscorrelation constraints are satisfied or not.

The number of codewords for a given length is small for smaller values of λ_a and λ_c, therefore, sometimes it is required to relax the performance requirement a little bit to accomodate a large number of users. We can use iterative methods [32] to construct new codes from given codes. For example:

1) Given an $(n, w, \lambda_a, \lambda_c)$ code C, we can construct a $(n, w, \lambda_A, \lambda_C)$ code C', with $\lambda_A \geq \lambda_a$, $\lambda_C \geq \lambda_c$.

2) Given an $(n, w, \lambda_a, \lambda_c)$ code C with M codewords, we can construct a code C' with $\binom{M}{2}$ codewords with parameters $(n, 2w - 2\lambda_c, 2\lambda_a + 2\lambda_c, w + 3\lambda_c)$.

3) Given an $(n, w, \lambda_a, \lambda_c)$ code C, we can construct a $(tn, tw, tw, t\lambda_c)$ code C' with same number of codewords by concatenating t copies of each codeword of C.

A technique to construct $(n, w, 1, 2)$ codes, with twice as many codewords as in the $(n, w, 1, 1)$ codes, is given in [64].

Marić proposed OOCs based on Welch Costas arrays as described in [65]. These $(p(2p-3), p, 1, 1)$ codes have been referred to as Truncated Costas codes and can be constructed for any prime number p.

Yang et. al. presented a construction technique for unequal values of autocorrelation and crosscorrelations [66]. These are $(n, w, \lambda{+}m, \lambda)$ codes and can be constructed for a prime $n \equiv 1 \pmod{12}$.

A variable weight OOC (n, W, L, λ_c, Q) was proposed by Yang [67]. Here W is the set of different weights w_i, L is the set of λ_a^i and Q is the set of q_i, where q_i is the number of codewords of weight w_i.

The construction of OOCs using disjoint difference sets and triangles has been discussed in [32, 59, 68].

2.9 Discussion

In this section, we briefly compare the OOCs described in this Chapter on the basis of their code parameters.

The problem with the Prime Sequence codes, the "Quasi-Prime" codes and the Quadratic Congruence codes is that the number of codewords does not increase in proportion to the increased length of the codewords. For example, an increase in length from 25 to 121 in Prime Sequence codes results in the number of codewords increasing from 5 to 11 only. The same holds for the other two codes also. Therefore, even to have a moderate number of users in the optical CDMA system, we will have to use a very high chip rate. Here the codes based on $PG(m, q)$ have a distinct advantage because optimal codes can be constructed for $s = 1$ when m is even.

For the Prime Sequence codes and the "Quasi-Prime" codes, since the off-peak autocorrelation λ_a is almost as high as the peak of the autocorrelation value, this might create difficulties in establishing chip synchronization at the receiver. The Quadratic Congruence codes alleviate this difficulty, but, at the expense of tolerating (i) a high value of the crosscorrelation λ_c, and (ii) a reduction in the number of codewords by one.

We see that the maximum crosscorrelation λ_c is independent of code length for the Prime Sequence code. For the Quadratic Congruence code, both the autocorrelation and crosscorrelation constraints do not depend on code length. This means that as the code length n increases, or as the autocorrelation peak w increases, the crosscorrelation peak remains at a constant level. Consequently, it results in a better detection performance.

For $PG(m, q)$ codes, the code weight w (consequently, the autocorrelation peak) and the correlation constraints (λ_a, λ_c) do not depend on the code length for a fixed q. Instead, λ_a and λ_c depend on the value of s chosen. We can obtain a large number of codewords for a given length of codewords, but the construction procedure is involved.

A larger length of the codewords significantly limits the data rates that can be supported. The practical constraints on the minimum possible laser pulse width, and the requirement to support higher data rates, necessitate that the lengths of codewords should not increase indefinitely even when we want to maximize the number of users. Two dimensional coding, such as coding in Temporal/Spatial codes, reduces the temporal length of the codewords and the number of users is increased by using more than one spatial channel.

The 2^n Prime Sequence codes are a variant of the Prime Sequence codes and are amenable to generation by a serial coding structure involving 2 x 2 couplers and delay lines. This reduces power losses during encoding and decoding. The maximum off-peak autocorrelation value λ_a and the maximum crosscorrelation value λ_c are never worse than those of the Prime Sequence codes. However, the number of codewords is lesser than that of Prime Sequence code of the same length.

OOCs using constant weight error correcting codes give a large number of codewords for a given length. The usefulness of this method lies in the fact that we can obtain OOCs for any given integer values of correlation λ, and weight of the codewords w. All we need is a constant weight error correcting code with minimum distance $d \geq 2(w - \lambda)$.

In the next three chapters, we propose some new classes of OOCs that give larger number of codewords for a given code length.

Chapter 3

Optical Orthogonal Codes using Hadamard Matrices

In this chapter, we discuss a method of generating Optical Orthogonal Codes using the well known Hadamard matrices. We begin by briefly introducing the required mathematical background on difference sets and Hadamard matrices. Later, we present a construction technique for Optical Orthogonal Codes using these Hadamard matrices and illustrate the technique through suitable examples. We also present the properties of the proposed OOCs [69].

3.1 Difference Sets

In this section, we briefly review basics of difference families and difference sets[1]. Much of the reference material on difference families is taken from [70].

Definition 3.1.1 [70]

Let G be an additive abelian group of order n. Then t w-element subsets of G, $B_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,w}\}$, *where* $1 \leq i \leq t$, form a (n, w, λ) *difference family* (also called difference system) if every nonzero element of G occurs λ times among the differences $\{b_{i,x} - b_{i,y}\}$, *where* $\{i = 1, 2, \ldots, t; \;\; x, y = 1, 2, \ldots, w\}$. The sets B_i are called *base blocks.*

[1] Appendix A gives a somewhat more detailed exposition of difference sets and difference families.

Table 3.1.1: Base blocks of a $(n, 3, 1)$ difference family

n	Base Block
7	(0,1,3)
13	(0,1,4) (0,2,7)
15	(0,1,4) (0,2,9) (0,5,10)

If $t = 1$, then B_i is an abelian difference set (n, w, λ).

If $B_1, B_2, \ldots, B_t$ form a (n, w, λ) difference family, then the translates of the base blocks, namely $B_i+g = \{b_{i,1}+g, b_{i,2}+g, \ldots, b_{i,w}+g\}$, *where* $\{i = 1, 2, \ldots, t,\ g \in G\}$, forms a (n, w, λ) *Balanced Incomplete Block Design* (BIBD).

Definition 3.1.2 [71]

A set of w residues $D : \{a_1, a_2, \ldots, a_w\}$ modulo n is called a (n, w, λ) difference set if for every $d \neq 0$ (modulo n), there are exactly λ ordered pairs (a_i, a_j) and $(a_i, a_j) \in D$ such that $(a_i - a_j) = d$ (modulo n).

Theorem 3.1.1 [71]

A set of w residues $D : \{a_1, a_2, \ldots, a_w\}$ modulo n is a (n, w, λ) difference set if and only if the sets $B_i : \{a_1 + i, a_2 + i, \ldots, a_w + i\}$ modulo n, $i = 1, 2, \ldots, n-1$ are a cyclic (n, w, λ) block design B.

Examples of difference families of type $(n, 3, 1)$ and their base blocks are shown in Table 3.1.1.

Theorem 3.1.2 [71]

If there is a (n_i, w, λ_i) difference family, then through suitable interplay between n_i and λ_i, a different sized difference family can be generated.

3.2 Hadamard Matrices

Hadamard matrices [72] were first studied by Sylvester in 1867. In 1893, Hadamard discovered that if $H = (h_{ij})$ is a matrix of order n, then

$$|det\, H|^2 \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |h_{ij}|^2 \qquad (3.2.1)$$

Hadamard showed that the matrices satisfying the equality and with entries in the unit disc (i.e., $|h_{ij}| \leq 1$) have order 1,2, or 0 (mod 4) and entries (1,-1). A Hadamard matrix H therefore satisfies

$$H\, H^t = nI \qquad (3.2.2)$$

i.e., its rows are pairwise orthogonal.

The pairwise orthogonality properties of the Hadamard matrices have been investigated in a wide variety of fields for a variety of applications such as

- Statistics: Hadamard matrices have been used to construct symmetric balanced incomplete block designs and optimal weighing designs.

- Information theory and signal processing: Hadamard matrices are used to generate codes which correct maximum possible number of errors and some sequences of use in digital communications.

In this chapter, we discuss a method of using Hadamard matrices to contruct Optical Orthogonal Codes for use in an optical CDMA environment.

A Hadamard matrix of order 2, denoted by H_2, is represented as

$$H_2 = \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix} \qquad (3.2.3)$$

In general, a Hadamard matrix of order H_{2n} can be constructed using a Hadamard matrix of order H_n in the following fashion:

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix} \qquad (3.2.4)$$

where $-H_n$ means complement of H_n. Hadamard matrices exist[2] for certain orders only.

In our work, we will assume that a Hadamard matrix exists for the particular order, i.e., we will not concentrate on the construction of Hadamard matrices. There is a large literature available on various methods of construction of Hadamard matrices [70].

Our interest is to derive Optical Orthogonal Codes using these Hadamard matrices (assuming that the Hadamard matrices for corresponding order exist) and to ascertain their correlation parameters.

3.3 Construction of OOCs

As described in Chapters 1 and 2, the positivity of the optical correlator makes us to think of only those sequences which are truly (0,1) instead of (1,-1) for use in the incoherent optical CDMA systems.

Without any loss of generality, we replace all -1's in a Hadamard matrix by 0's and keep +1's as 1's.

Therefore, the Hadamard matrix of order 2 in equation 3.2.3 becomes:

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad (3.3.1)$$

The approach we follow here is to consider Hadamard matrices having entries as (0,1) and try to relate them to difference sets. Then we impose the periodicity constraints required for OOCs to obtain a new family of Optical Orthogonal Codes based on Hadamard matrices.

From a Hadamard matrix of order n, we write a truncated Hadamard matrix of order $(n-1)$ by deleting the first row and the first column. Then we write all rows

[2] Necessary conditions and existence conjectures are briefly summarized in Appendix B.

(in fact, we can also write all columns) in the form of difference sets, i.e., we write the rows in the form of w-sets. We consider the cyclic shifts of a codeword as the same codeword.

Proposition 3.3.1 *For Optical Orthogonal Codes constructed using Hadamard matrices of order n, the codewords corresponding to w-sets B_1 and $B_{(n+1)/2}$ have an off-peak autocorrelation equal to $(n-2)$.*

This is because, a Hadamard matrix of order H_{2n} is constructed from a Hadamard matrix of order H_n, and in the way 1's and 0's are distributed in a Hadamard matrix. In practice, the codewords corresponding to w-sets B_1 and $B_{(n+1)/2}$ should not be used. We have listed the properties of Optical Orthogonal Codes using Hadamard matrices, excluding these two codewords.

We illustrate the concept through two examples.

Example 3.3.1: OOCs USING HADAMARD MATRIX OF ORDER = 8

Let us write a Hadamard matrix of order $n = 8$.

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \tag{3.3.2}$$

After deleting the first row and the first column, the truncated matrix becomes:

$$H_{7(truncated)} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \tag{3.3.3}$$

Now we write the rows in terms of w-sets as

B_1 = {1,3,5}

B_2 = {0,3,4}

B_3 = {2,3,6}

B_4 = {0,1,2}

B_5 = {1,4,6}

B_6 = {0,5,6}, and

B_7 = {2,4,5}

The periodicity checks, wherein we disallow those codewords that can be obtained as the cyclic shifts of other codewords, render only B_1, B_2, B_4 and B_7 into valid w-sets of Optical Orthogonal Code constructed using Hadamard matrices. We have four codewords C_1, C_2, C_3 and C_4 corresponding to these four valid w-sets.

The codewords of the Optical Orthogonal Code thus generated are:

C_1 = {0 1 0 1 0 1 0}

C_2 = {1 0 0 1 1 0 0}

C_3 = {1 1 1 0 0 0 0}, and

C_4 = {0 0 1 0 1 1 0}

As pointed out in Proposition 3.3.1, the codewords corresponding to B_1 and B_4 should not be used. The corresponding codewords C_1 and C_3 are not used as they have a very high off-peak autocorrelation.

The properties of this code are:

1. Length of the codewords, $n = 7$
2. Weight of the codeword, $w = 3$
3. The maximum value of off-peak autocorrelation, $\lambda_a = 1$
4. The maximum value of crosscorrelation, $\lambda_c = 2$

Therefore, this is a (7,3,1,2) code with two usable codewords C_2 and C_4.

The autocorrelation of codeword C_2 and C_4 of example 3.3.1 is shown in Fig. 3.3.1

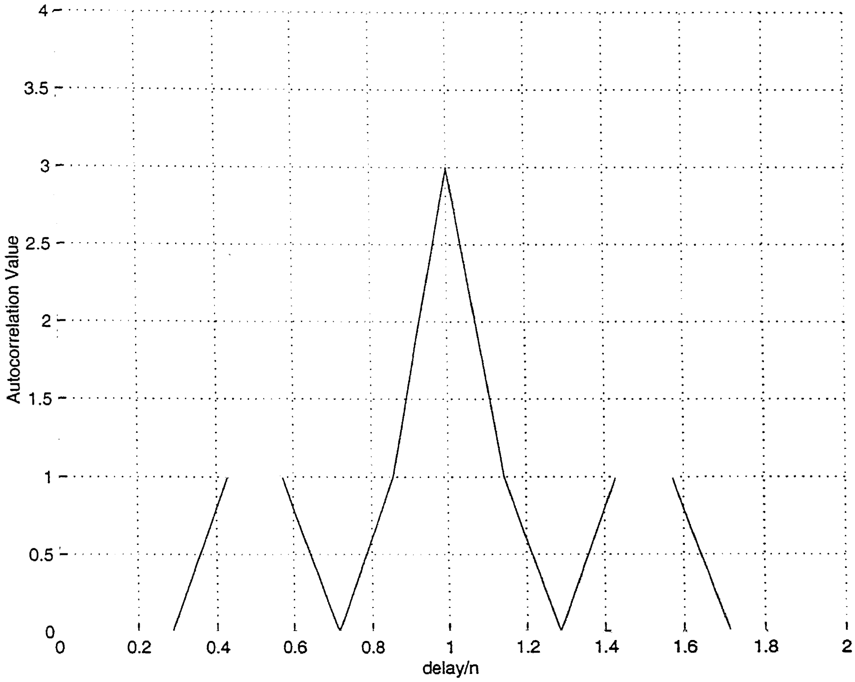

Figure 3.3.1: Autocorrelation of codeword C_2 of a (7,3,1,2) OOC based on Hadamard Matrices

and Fig. 3.3.2, respectively. As can be seen from Figs. 3.3.1 and 3.3.2, the peak value of autocorrelation is equal to the weight of the code (which is 3 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value does not exceed 1 in the plots. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_2 and C_4 of example 3.3.1 is shown in Fig. 3.3.3. As can be seen from Fig. 3.3.3, the maximum crosscorrelation value between the two codewords never exceeds 2.

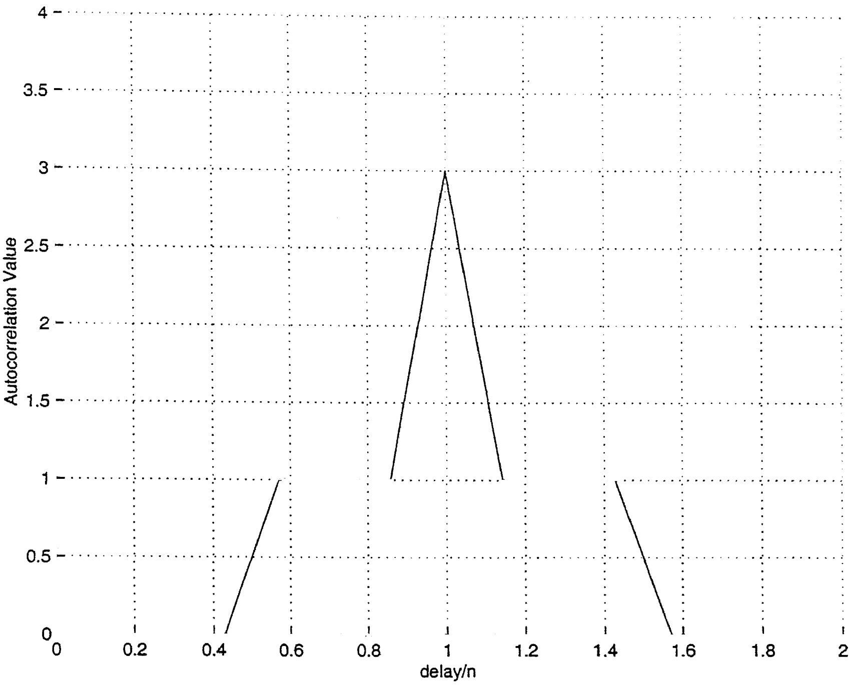

Figure 3.3.2: Autocorrelation of codeword C_4 of a (7,3,1,2) OOC based on Hadamard Matrices

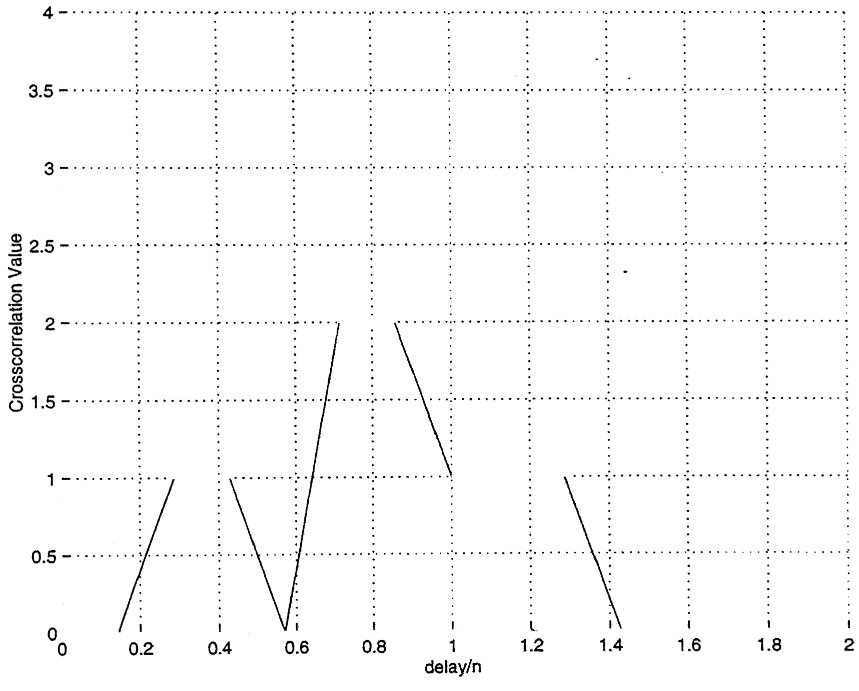

Figure 3.3.3: Crosscorrelation between codeword C_2 and codeword C_4 of a (7,3,1,2) OOC based on Hadamard Matrices

Example 3.3.2: OOCs USING HADAMARD MATRIX OF ORDER = 16

First we write a Hadamard matrix of order $n = 16$.

$$H_{16} = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1\\
1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&0&1&0&0&1&0&1&1&0&1&0&0&1&0&1\\
1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1\\
1&0&0&1&0&1&1&0&1&0&0&1&0&1&1&0\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1\\
1&1&0&0&1&1&0&0&0&0&1&1&0&0&1&1\\
1&0&0&1&1&0&0&1&0&1&1&0&0&1&1&0\\
1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1\\
1&0&1&0&0&1&0&1&0&1&0&1&1&0&1&0\\
1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0\\
1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1
\end{pmatrix} \tag{3.3.4}$$

After deleting the first row and the first column, the truncated matrix becomes:

$$H_{15(truncated)} = \begin{pmatrix}
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
1&0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1\\
1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
0&1&0&0&1&0&1&1&0&1&0&0&1&0&1\\
1&0&0&0&0&1&1&1&1&0&0&0&0&1&1\\
0&0&1&0&1&1&0&1&0&0&1&0&1&1&0\\
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
0&1&0&1&0&1&0&0&1&0&1&0&1&0&1\\
1&0&0&1&1&0&0&0&0&1&1&0&0&1&1\\
0&0&1&1&0&0&1&0&1&1&0&0&1&1&0\\
1&1&1&0&0&0&0&0&0&0&0&1&1&1&1\\
0&1&0&0&1&0&1&0&1&0&1&1&0&1&0\\
1&0&0&0&0&1&1&0&0&1&1&1&1&0&0\\
0&0&1&0&1&1&0&0&1&1&0&1&0&0&1
\end{pmatrix} \tag{3.3.5}$$

We write the rows in terms of w-sets as

$B_1 = \{1,3,5,7,9,11,13\}$

$B_2 = \{0,3,4,7,8,11,12\}$

$B_3 = \{2,3,6,7,10,11,14\}$

$B_4 = \{0,1,2,7,8,9,10\}$

$B_5 = \{1,4,6,7,9,12,14\}$

$B_6 = \{0,5,6,7,8,13,14\}$

$B_7 = \{2,4,5,7,10,12,13\}$

$B_8 = \{0,1,2,3,4,5,6\}$

$B_9 = \{1,3,5,8,10,12,14\}$

$B_{10} = \{0,3,4,9,10,13,14\}$

$B_{11} = \{2,3,6,8,9,12,13\}$

$B_{12} = \{0,1,2,11,12,13,14\}$

$B_{13} = \{1,4,6,8,10,11,13\}$

$B_{14} = \{0,5,6,9,10,11,12\}$, and

$B_{15} = \{2,4,5,8,9,11,14\}$

The periodicity checks, wherein we disallow those codewords that can be obtained as the cyclic shifts of other codewords, render only B_1, B_2, B_4, B_5, B_7, B_8, B_{10}, B_{11}, B_{13}, B_{14}, and B_{15} into valid w-sets. We have eleven codewords C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10}, and C_{11} corresponding to these eleven valid w-sets.

The codewords of the Optical Orthogonal Code thus generated are:

$C_1 = \{0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\}$

$C_2 = \{1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\}$

$C_3 = \{1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\}$

$C_4 = \{0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\}$

$C_5 = \{0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\}$

$C_6 = \{1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\}$

$C_7 = \{1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\}$

$C_8 = \{0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\}$

$C_9 = \{0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,1\,0\}$

$C_{10} = \{1\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\}$

$C_{11} = \{0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,0\,1\}$

As pointed out in Proposition 3.3.1, the codewords corresponding to B_1 and B_8 should not be used. The corresponding codewords C_1 and C_6 are not used as they have a very high off-peak autocorrelation.

The properties of this code are:

1. Length of the codeword, $n = 15$
2. Weight of the codeword, $w = 7$
3. The maximum value of off-peak autocorrelation, $\lambda_a = 3$
4. The maximum value of crosscorrelation, $\lambda_c = 4$

Therefore, this is a (15,7,3,4) code.

The autocorrelation of codeword C_3, C_7, and C_{10} of example 3.3.2 is shown in Figs. 3.3.4, 3.3.5, and 3.3.6, respectively. As can be seen from Figs. 3.3.4, 3.3.5 and 3.3.6, the peak value of autocorrelation is equal to the weight of the code (which is 7 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) does not exceed 3 in the plots.

The crosscorrelation between codewords C_{10} and C_2 of example 3.3.2 is shown in Fig. 3.3.7. The crosscorrelation between codewords C_3 and C_7 is shown in Fig. 3.3.8. Fig. 3.3.9 shows the crosscorrelation between codewords C_{10} and C_2. As can be seen from Figs. 3.3.7 - 3.3.9, the maximum crosscorrelation value between any two codewords never exceeds 4.

3.4 Generalized Construction Procedure

An Optical Orthogonal Code using Hadamard matrices can be constructed in the following steps:

1. Take a normalized Hadamard matrix of order $n+1 = 4t$, where n is the length of the code and t an integer.
2. By deleting the first row and the first column, construct a truncated Hadamard

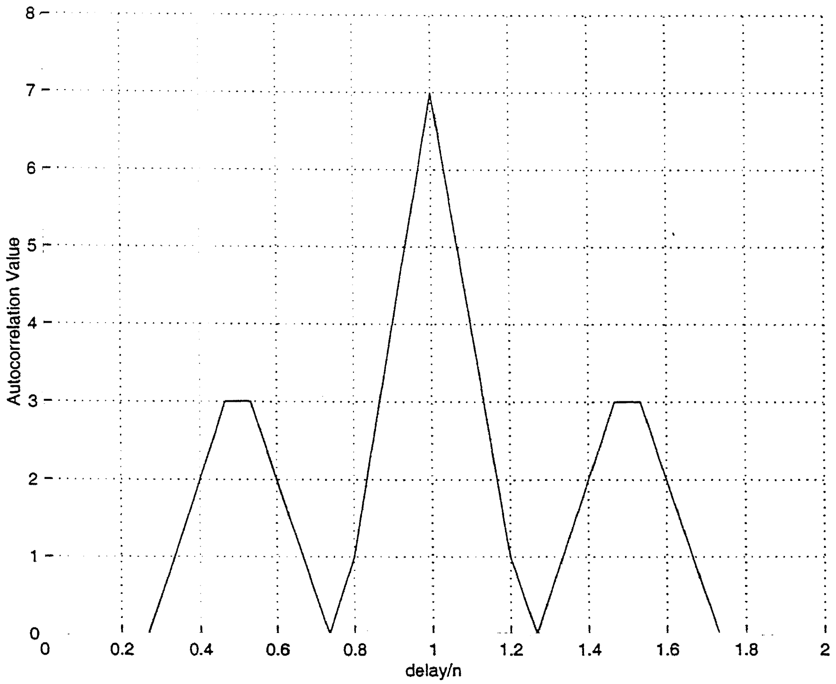

Figure 3.3.4: Autocorrelation of codeword C_3 of a (15,7,3,4) OOC based on Hadamard Matrices

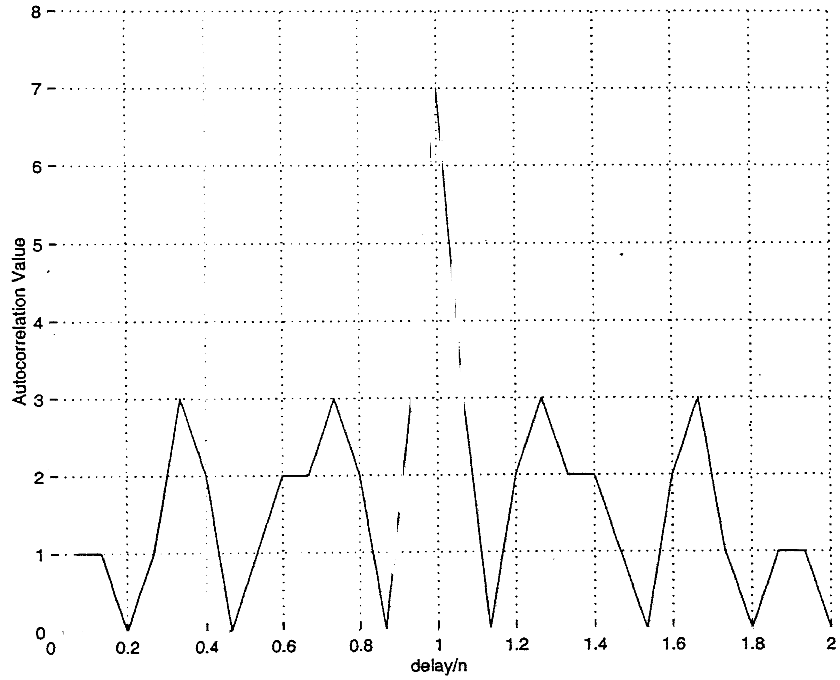

Figure 3.3.5: Autocorrelation of codeword C_7 of a (15,7,3,4) OOC based on Hadamard Matrices

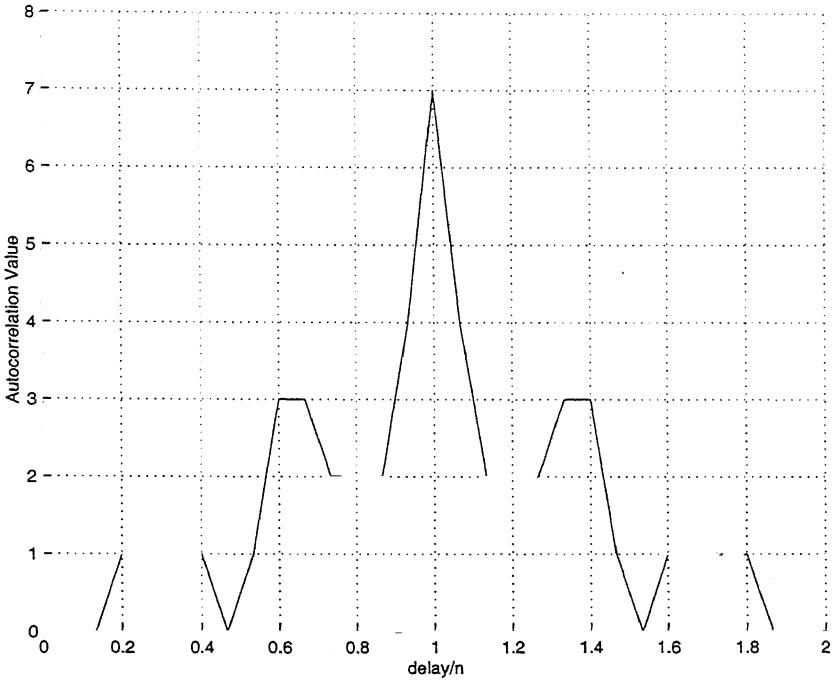

Figure 3.3.6: Autocorrelation of codeword C_{10} of a (15,7,3,4) OOC based on Hadamard Matrices

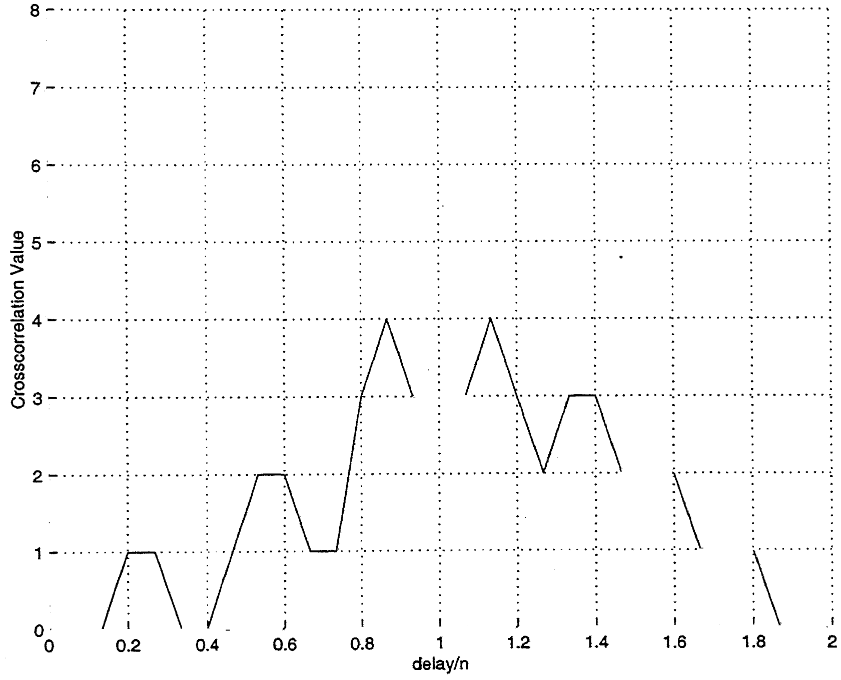

Figure 3.3.7: Crosscorrelation between codeword C_{10} and codeword C_2 of a (15,7,3,4) OOC based on Hadamard Matrices

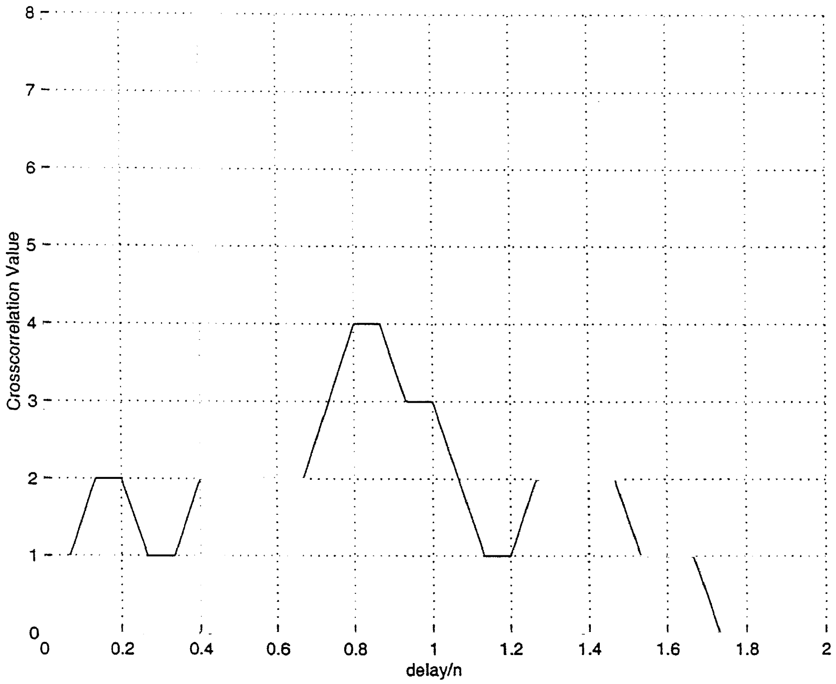

Figure 3.3.8: Crosscorrelation between codeword C_3 and codeword C_7 of a (15,7,3,4) OOC based on Hadamard Matrices

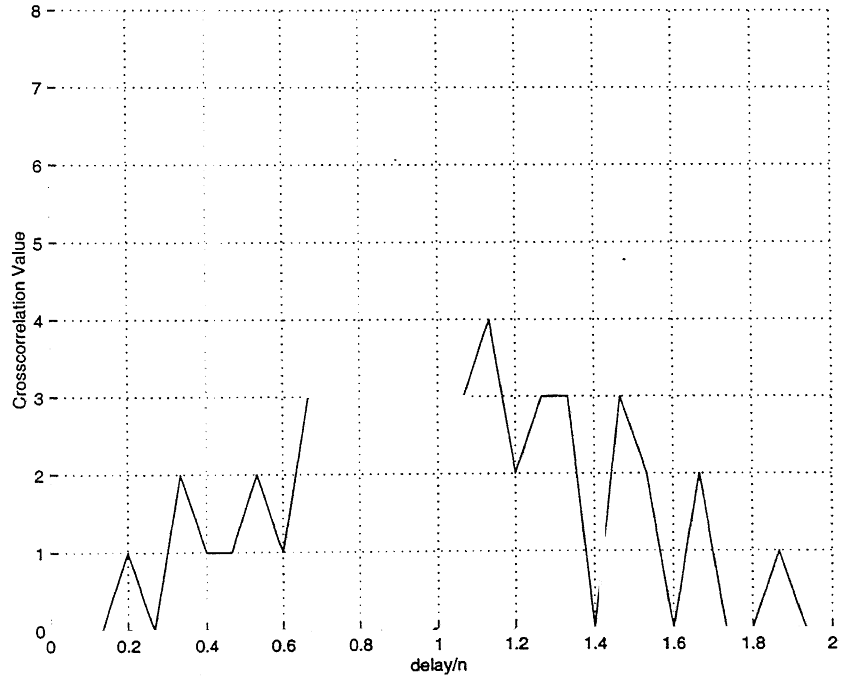

Figure 3.3.9: Crosscorrelation between codeword C_{11} and codeword C_4 of a (15,7,3,4) OOC based on Hadamard Matrices

matrix. The order of this matrix is n. This matrix is not Hadamard in nature.

3. Now represent all rows (or all columns) in the form of a w-set, by knowing the positions of 1's.

4. Then check for the periodicity properties of the w-sets. Remove those w-sets, which can be obtained as cyclic shifts of other w-sets formed in Step 3. This is done because, in OOCs the cyclic shift of a codeword is considered the same as the codeword itself in case of asynchronous optical CDMA systems.

5. Now we consider the remaining w-sets of Step 4. For Optical Orthogonal Codes constructed using truncated Hadamard matrices of order n, the codewords corresponding to w-sets B_1 and $B_{(n+1)/2}$ have a large off-peak autocorrelation of $(n-2)$. Therefore, in practice, the codewords corresponding to w-sets B_1 and $B_{(n+1)/2}$ should not be used.

6. Finally, the w-sets remaining after Step 5 constitute the codewords of the constructed code.

3.5 Discussion

A new class of Optical Orthogonal Codes based on Hadamard matrices has been presented in this chapter. The properties of the OOCs discussed in this chapter are:

- Length of the codeword $n = 4t - 1$
- Weight of the code $w = 2t - 1$
- The maximum value of off-peak autocorrelation, $\lambda_a = t - 1$
- The maximum value of crosscorrelation, $\lambda_c = t$

The codewords of length n of this class of Optical Orthogonal Codes are derived from a Hadamard matrix of order $(n+1)$. A generalized construction technique for this class of codes has been presented in section 3.4.

We have illustrated the construction technique with the help of two examples, one using H_8 and the other H_{16}. The resultant codewords have been listed for the two cases.

The autocorrelation and crosscorrelation functions for the codewords of the codes (7,3,1,2) and (15,7,3,4) have been plotted. The plots show that the correlation constraints never exceed the values given by code parameters.

Whereas a Prime Sequence code can be generated for every prime number, the design of OOCs here is constrained by the existence of Hadamard matrices of an appropriate size.

In the next chapter, we discuss the construction of OOCs using Skolem Sequences.

Chapter 4

Optical Orthogonal Codes using Skolem Sequences

In this chapter, we present a method of constructing a class of Optical Orthogonal Codes using Skolem Sequences. Here we use the fact that for any w-set $\{x_1, x_2, \ldots, x_w\}$, there are $w(w-1)/2$ total differences between the positions of 1's. The basic idea here is to put the integers in a w-set in such a way that $w(w-1)/2$ differences are all distinct.

The Skolem sequences [70] of an order n provide n pairs of two elements each, such that differences between the two elements of every pair are distinct. We use Skolem sequences in our task of uniquely placing the integers in the w-set to construct a class of OOCs.

4.1 Distances in w-sets

In set theoretic notation, a codeword X in C is represented as a w-set by $X = \{x_1, x_2, \ldots, x_w\}$, where w is the weight of the codeword, and x_i's represent positions of 1's within the codeword.

Now the differences $x_j - x_i$, $\{1 \leq i, j \leq w\}$ for a w-set are equal to

$x_2 - x_1,\ x_3 - x_2,\ x_4 - x_3, \ldots,\ x_w - x_{w-1},$

$x_3 - x_1,\ x_4 - x_2,\ x_5 - x_3, \ldots,\ x_w - x_{w-2},$

$x_4 - x_1,\ x_5 - x_3,\ x_6 - x_3, \ldots,\ x_w - x_{w-3}$ etc.

The total number of differences is $w(w-1)/2$. For example, when w=5, the total number of differences is $5(5-1)/2$=10.

Here all the differences are expressed modulo n, where n is the total length of the code sequence. This is done for maintaining the periodicity and cyclic property of the codes. As is obvious, the minimum length possible for any codeword is $(x_w - x_1) + 1$.

Theorem 4.1.1 *The minimum value of code length n required to generate M codewords, each with weight w and correlation parameters* $\lambda = \lambda_a = \lambda_c = 1$, *is given by*

$$n \geq w(w-1)M + 1 \tag{4.1.1}$$

Proof: From the Johnson Bound [73], total number of codewords for $(n, w, \lambda_a, \lambda_c)$ code, with $\lambda = max(\lambda_a, \lambda_c)$, is equal to

$$M \leq \frac{(n-1)\ldots(n-\lambda)}{w(w-1)(w-2)\ldots(w-\lambda)} \tag{4.1.2}$$

For $\lambda = \lambda_a = \lambda_c = 1$, equation 4.1.2 becomes

$$M \leq \frac{(n-1)}{w(w-1)} \tag{4.1.3}$$

which gives $n \geq w(w-1)M + 1.\square$

The minimum length required to generate M codewords, each having a weight 3, is equal to $6M + 1$.

In a w-set, by knowing the adjacent distances, all other distances can be calculated. We illustrate this with the help of following examples.

Example 4.1.1: w=3 CASE

Let us take, for simplicity, a codeword with only 3 elements, i.e., w=3. So we have $X = \{x_1, x_2, x_3\}$.

Therefore, all the distances are $x_2 - x_1$, $x_3 - x_2$ and $x_3 - x_1$.

But $(x_3 - x_1) = (x_2 - x_1) + (x_3 - x_2)$. This means that we need to know only the adjacent distances. The same example can be applied to any w. All other distances can then be obtained by knowing the adjacent distances.

Example 4.1.2: w=4 CASE

Total number of distinct distances are $4(4-1)/2 = 6$, out of which three are adjacent distances. These are $x_2 - x_1$, $x_3 - x_2$ and $x_4 - x_3$. Other distances can be obtained from these first order distances as follows:

$(x_3 - x_1) = (x_2 - x_1) + (x_3 - x_2)$

$(x_4 - x_2) = (x_3 - x_2) + (x_4 - x_3)$, and

$(x_4 - x_1) = (x_2 - x_1) + (x_3 - x_2) + (x_4 - x_3)$

4.2 Mathematical Formulation

For each w-set, there are $w(w-1)/2$ distinct distances. The M codewords each having weight w, can be represented as M w-sets. We write the set of M w-sets as

$$\{x_{i1}, x_{i2}, \ldots, x_{iw}\}, \quad \text{where } 1 \leq i \leq M. \tag{4.2.1}$$

Here x_{ij} represents position of the j^{th} 1 in the i^{th} codeword. To generate an OOC, we need to put suitable values in the above M w-sets.

Example 4.2.1: CODEWORDS WITH w=3

For the design of codewords with weight w=3, we have the M 3-sets as follows:

$\{x_{i1}, x_{i2}, x_{i3}\}$ for $1 \leq i \leq M$.

Here x_{i1} represents the position of the first 1 in the i^{th} codeword, and so on. There are three elements in every set, as each codeword has weight w=3.

Let us now represent distances between 1's in the 3-sets as

$x_{i(2,1)} = x_{i2} - x_{i1}$,

$x_{i(3,1)} = x_{i3} - x_{i1}$, and

$x_{i(3,2)} = x_{i3} - x_{i2}$

In the above expression, $x_{i(k,j)}$ represents the distance between the k^{th} 1 and the j^{th} 1 in the w-set corresponding to the i^{th} codeword. For simplicity, let us put a 1 in the zeroth position and then try to search for positions of other 1's in each 3-set. So $x_{i1} = 0$, $x_{i(2,1)} = x_{i2}$, $x_{i(3,1)} = x_{i3}$, and $x_{i(3,2)} = x_{i3} - x_{i2}$.

Here

$$x_{i(3,1)} = x_{i(3,2)} + x_{i(2,1)} \text{ for } 1 \leq i \leq M \tag{4.2.2}$$

Since we want all the distances in equation 4.2.2 to be unique for M codewords, we require a minimum size of the integer set equal to 3M. As long as we are able to find integers from the integer set $\{1, 2, \ldots, 3M\}$ to satisfy equation 4.2.2, our problem of finding M 3-sets is solved.

Theorem 4.2.1 *3M diferent numbers {1,2,..., 3M} can be partitioned into M different 3-sets only when M = 0 (mod 4) or M = 1 (mod 4).*

Proof:

Equation 4.2.2 can also be written as

$$\sum_{i=1}^{M} x_{i(3,1)} = \sum_{i=1}^{M} (x_{i(3,2)} + x_{i(2,1)}) \tag{4.2.3}$$

Since we are having 3M disjoint numbers $\{x_{i(3,1)}, x_{i(3,2)}, x_{i(2,1)}\}$ with $1 \leq i \leq M$, therefore, we have

$$\sum_{i=1}^{M} (x_{i(2,1)} + x_{i(3,2)} + x_{i(3,1)}) = \sum_{i=1}^{3M} i \tag{4.2.4}$$

So we have from the above three equations (4.2.2, 4.2.3 and 4.2.4)

$$\sum_{i=1}^{M} x_{i(3,1)} = 1/2 \sum_{i=1}^{3M} i = \frac{3M(3M+1)}{4} \tag{4.2.5}$$

Since the LHS of equation 4.2.5 is an integer, the RHS also has to be an integer. Therefore, the above equation implies that either M = 0 (mod 4) or 1 (mod 4).□

4.3 Construction of Codes

In this section, we discuss the construction of codes. In the previous section, we placed a 1 in the 0^{th} position to solve equation 4.2.2 for M different 3-sets. Now we consider the positioning of the second 1 in the M 3-sets.

Let us take $x_{i(2,1)} = i$. If $i = 1, 2, \ldots, M$, and we are able to find distinct values for $x_{i(3,2)}$ and $x_{i(3,1)}$ from the set of integers $\{1, 2, \ldots, 3M\}$ to solve equation 4.2.2, then our purpose of generating M codewords, each having a weight 3, is achieved. The i^{th} codeword is $\{0, i, x_{i(3,1)}\}$.

From equation 4.2.2,

$$x_{i(3,1)} - x_{i(3,2)} = x_{i(2,1)} = i \tag{4.3.1}$$

As we want $1 \leq i \leq M$, and since we have to choose unique distances from integer set $\{1, 2, \ldots, 3M\}$, therefore, we have a set of 2M values in the range $\{M+1, M+2, \ldots, 3M\}$ to choose the values for $x_{i(3,1)}$ and $x_{i(3,2)}$ on the LHS of equation 4.3.1.

Towards this end of finding suitable values on the LHS of equation 4.3.1, we make use of Skolem sequences[1] [70]. The Skolem sequences of an order n provide n pairs of two elements each, such that differences between the two elements of every pair are distinct.

[1] More details about the construction of the Skolem sequences are given in Appendix C.

4.3.1 Skolem Sequences

In this subsection, we briefly discuss the Skolem sequences and their properties relevant to the construction of OOCs.

Definition 4.3.1 A Skolem sequence of order n is a sequence $S = \{s_1, s_2, \ldots, s_{2n}\}$ of $2n$ integers satisfying the following conditions:

1. for every $k \in \{1, 2, \ldots, n\}$, there exists exactly two elements $S_i, S_j \in S$ such that $S_i = S_j = k$.

2. if $S_i = S_j = k$ with $i < j$, then $j - i = k$.

Skolem sequences are also written as a collection of ordered pairs $\{(a_i, b_i) : 1 \leq i \leq n, b_i - a_i = i\}$ with $\bigcup_{i=1}^{n}\{a_i, b_i\} = \{1, 2, \ldots, 2n\}$. Throughout this work, we use the ordered pair notation for Skolem sequences.

Example 4.3.1.1: Skolem sequence of order 5

A Skolem sequence of order 5 can be represented as a collection of ordered pairs in the following fashion:

$$S = \{(1,2)\ (7,9)\ (3,6)\ (4,8)\ (5,10)\}$$

Theorem 4.3.1 [70]

A Skolem sequence of order n exists if and only if $n \equiv 0 (mod\ 4)$ or $n \equiv 1 (mod\ 4)$.

Proof: We need to prove that we can always partition the numbers $\{1, 2, \ldots, 2M\}$ into M pairs $\{a_j, b_j\}$ such that

$$(b_j - a_j) = j \text{ for } 1 \leq j \leq M \tag{4.3.2}$$

Summing on both sides, we have

$$\sum_{j=1}^{M}(b_j - a_j) = \sum_{j=1}^{M} j \tag{4.3.3}$$

As $\{a_j, b_j\}$ is a collection of numbers from the set $\{1, 2, \ldots, M\}$, therefore,

$$\sum_{j=1}^{M}(b_j + a_j) = \sum_{j=1}^{2M} j \tag{4.3.4}$$

Summation of the above two equations (4.3.3 and 4.3.4) yields

$$\sum_{j=1}^{M} b_j = 1/2\left\{\sum_{j=1}^{2M} j + \sum_{j=1}^{M} j\right\} \tag{4.3.5}$$

i.e.,

$$\sum_{j=1}^{M} b_j = \frac{M(5M+3)}{4} \tag{4.3.6}$$

The LHS of above equation is an integer, therefore RHS must also be an integer. For RHS to be an integer, $M \equiv 0 \pmod 4$ or $M \equiv 1 \pmod 4$.□

4.3.2 Construction of Codes - contd.

Let us now construct the codes for weight w=3.

From equation 4.3.1, for $1 \le i \le M$, we have

$$x_{i(3,1)} - x_{i(3,2)} = x_{i(2,1)} = i \tag{4.3.7}$$

So we take Skolem sequences and use them for generating M 3-sets, by writing $x_{i(3,1)}$ and $x_{i(3,2)}$ as Skolem sequences for corresponding $i+M$ since we need to choose the values of $x_{i(3,1)}$ and $x_{i(3,2)}$ on the LHS of equation 4.3.7 from amongst $\{M+1, M+2, \ldots, 3M\}$ or $M+\{1, 2, \ldots, 2M\}$ values. We use Skolem sequences for corresponding $i+M$. We get these values by using Skolem sequences for $\{1, 2, \ldots, 2M\}$ and adding M to each element of the Skolem sequence.

Example 4.3.2.1: Construction of code for M=4, w=3

The minimum length of codewords required to construct an OOC with 4 codewords, each codeword having a weight 3, is found using Theorem 4.1.1 and is equal to 25. First, we write the Skolem sequences of order M=4.

$$S = \{(1,2)\ (5,7)\ (3,6)\ (4,8)\}$$

Therefore,

$i = 1,\ x_{i(3,1)} = M + 2 = 6$ and $x_{i(3,2)} = M + 1 = 5$

$i = 2,\ x_{i(3,1)} = M + 7 = 11$ and $x_{i(3,2)} = M + 5 = 9$

$i = 3,\ x_{i(3,1)} = M + 6 = 10$ and $x_{i(3,2)} = M + 3 = 7$

$i = 4,\ x_{i(3,1)} = M + 8 = 12$ and $x_{i(3,2)} = M + 4 = 8$

Our codewords are of type $\{0, i, x_{i(3,1)}\}$, as defined in section 4.3. So we write the 4 w-sets constructed using this technique with weight w=3 as

B_1 = {0,1,6}

B_2 = {0,2,11}

B_3 = {0,3,10}

B_4 = {0,4,12}

The corresponding codewords are:

$C_1 = \{1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\}$

$C_2 = \{1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\}$

$C_3 = \{1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\}$

$C_4 = \{1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\}$

The autocorrelation of codewords C_2 and C_3 of example 4.3.2.1 are shown in Figs. 4.3.1 and 4.3.2, respectively. As can be seen from Figs. 4.3.1 and 4.3.2, the peak value of autocorrelation is equal to the weight of the code (which is 3 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value

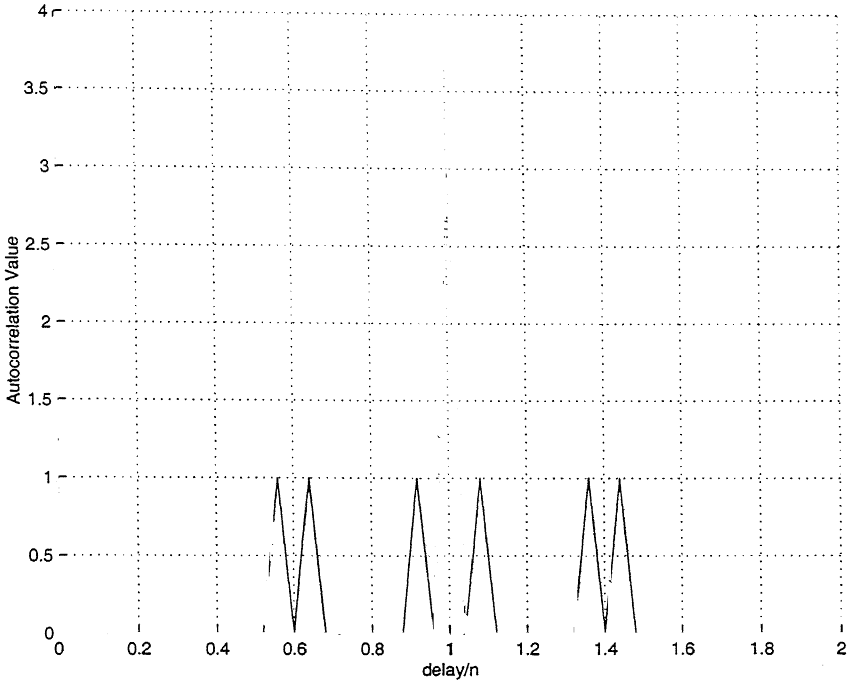

Figure 4.3.1: Autocorrelation of codeword C_2 of a (25,3,1,1) OOC based on Skolem Sequences

(side-lobe) in all the plots is equal to 1.

The crosscorrelation between codewords C_1 and C_4 of example 4.3.2.1 is shown in Fig. 4.3.3. The crosscorrelation between codewords C_2 and C_3 is shown in Fig. Fig. 4.3.4. As can be seen from Figs. 4.3.3 and 4.3.4, the maximum crosscorrelation value between any two codewords is equal to 1.

Example 4.3.2.2: CONSTRUCTION OF CODE FOR M=5, w=3

The minimum length of codewords required to construct an OOC with 5 codewords, each codeword having a weight 3, is obtained using Theorem 4.1.1 and is equal to 31. First we write the Skolem sequences of order M=5.

$$S = \{(1,2)\ (7,9)\ (3,6)\ (4,8)\ (5,10)\}$$

Therefore,

$i = 1$, $x_{i(3,1)} = M + 2 = 7$ and $x_{i(3,2)} = M + 1 = 6$

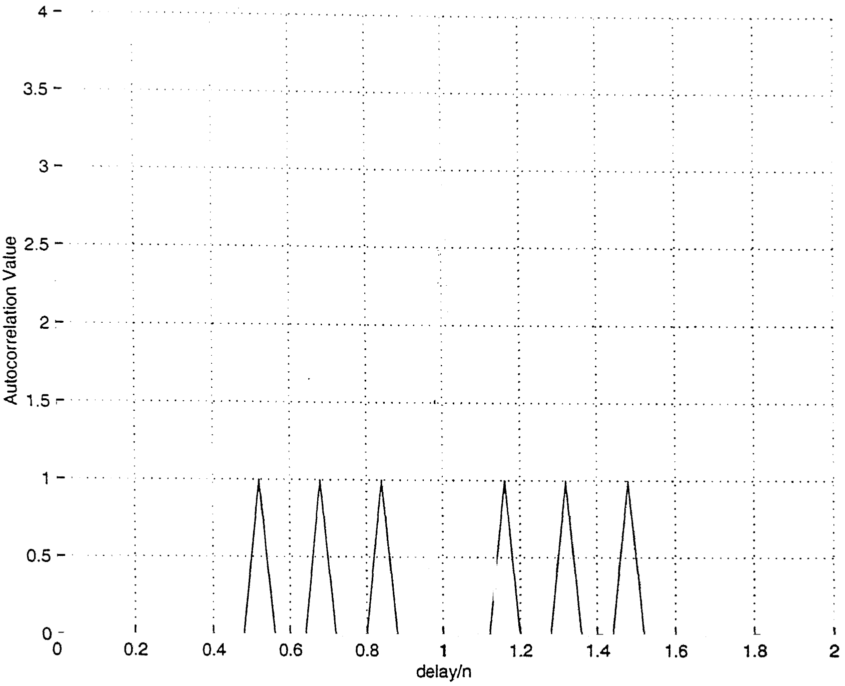

Figure 4.3.2: Autocorrelation of codeword C_4 of a (25,3,1,1) OOC based on Skolem Sequences

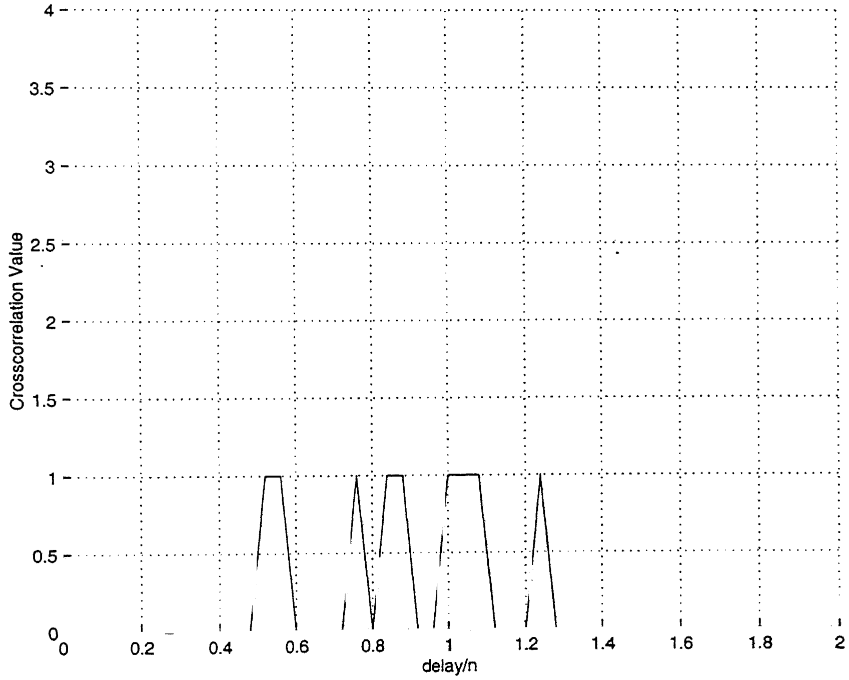

Figure 4.3.3: Crosscorrelation between codeword C_1 and codeword C_4 of a (25,3,1,1) OOC based on Skolem Sequences

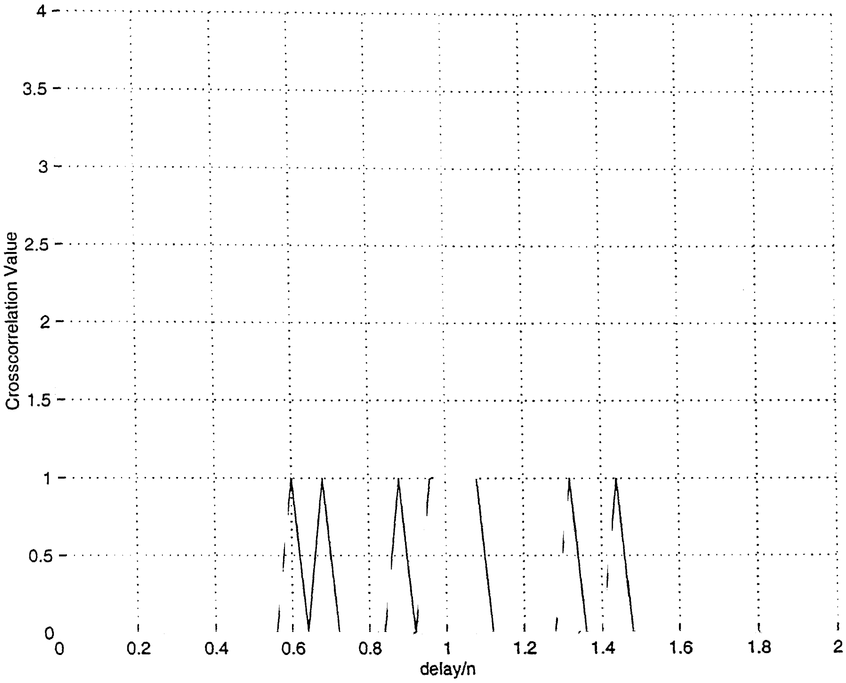

Figure 4.3.4: Crosscorrelation between codeword C_2 and codeword C_3 of a (25,3,1,1) OOC based on Skolem Sequences

$i = 2,\ x_{i(3,1)} = M + 9 = 14$ and $x_{i(3,2)} = M + 7 = 12$

$i = 3,\ x_{i(3,1)} = M + 6 = 11$ and $x_{i(3,2)} = M + 3 = 8$

$i = 4,\ x_{i(3,1)} = M + 8 = 13$ and $x_{i(3,2)} = M + 4 = 9$

$i = 5,\ x_{i(3,1)} = M + 10 = 15$ and $x_{i(3,2)} = M + 5 = 10$

Our codewords are of type $\{0, i, x_{i(3,1)}\}$, as defined in section 4.3. So we write the 5 w-sets constructed using this technique with weight w=3 as

$B_1 = \{(0,1,7\}$

$B_2 = \{0,2,14\}$

$B_3 = \{0,3,11\}$

$B_4 = \{0,4,13\}$

$B_5 = \{0,5,15\}$

The corresponding codewords are:

$C_1 = \{1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\}$

$C_2 = \{1010000000000001000000000000000\}$

$C_3 = \{1001000000010000000000000000000\}$

$C_4 = \{1000100000000100000000000000000\}$

$C_5 = \{1000010000000001000000000000000\}$

The autocorrelation of codewords C_1 and C_3 of example 4.3.2.2 are shown in Figs. 4.3.5 and 4.3.6, respectively. As can be seen from Figs. 4.3.5 and 4.3.6, the peak value of autocorrelation is equal to the weight of the code (which is 3 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) in all the plots is equal to 1. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_1 and C_3 of example 4.3.2.2 is shown in Fig. 4.3.7. The crosscorrelation between codewords C_2 and C_4 is shown in Fig. 4.3.8. As can be seen from Figs. 4.3.7 and 4.3.8, the maximum crosscorrelation value between any two codewords is equal to 1.

4.4 Generalized Construction Procedure

In this section, we present a generalized construction procedure to generate codewords of an OOC for a fixed weight of 3. An Optical Orthogonal Code of weight 3 can be constructed using Skolem sequences in the following steps:

1. Choose the number of codewords, M, to be constructed. All the codewords are of weight 3. The number of codewords must satisfy either $M \equiv 0 \mod 4$, or $M \equiv 1 \mod 4$.

2. The length of the codewords, $n = 6M + 1$.

3. Write the M 3-sets in the form of $\{x_{i1}, x_{i2}, x_{i3}\}$ for $1 \leq i \leq M$.

4. Place a 1 in the 0^{th} position of all 3-sets.

5. For the i^{th} 3-set, place a 1 in the i^{th} position.

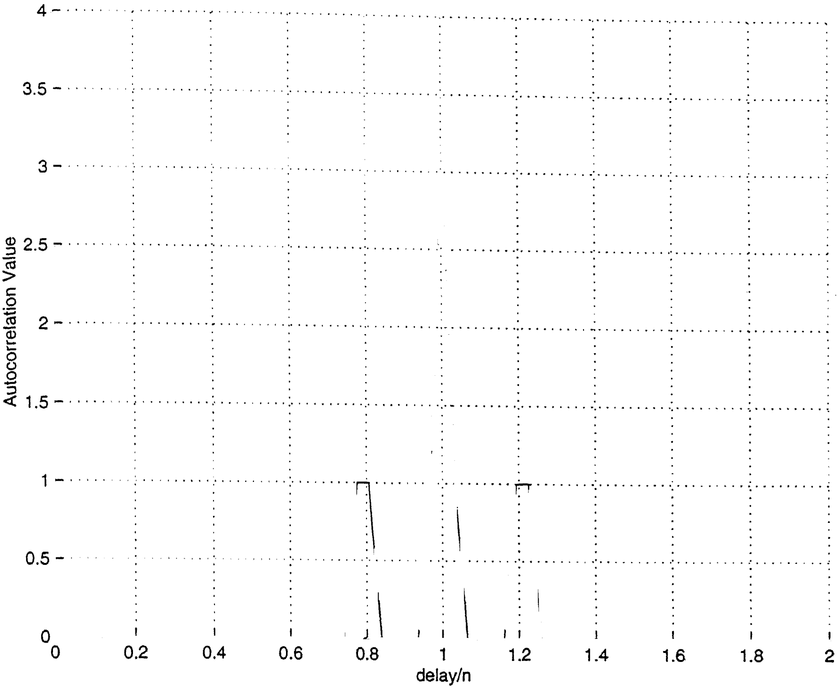

Figure 4.3.5: Autocorrelation of codeword C_1 of a (31,3,1,1) OOC based on Skolem Sequences

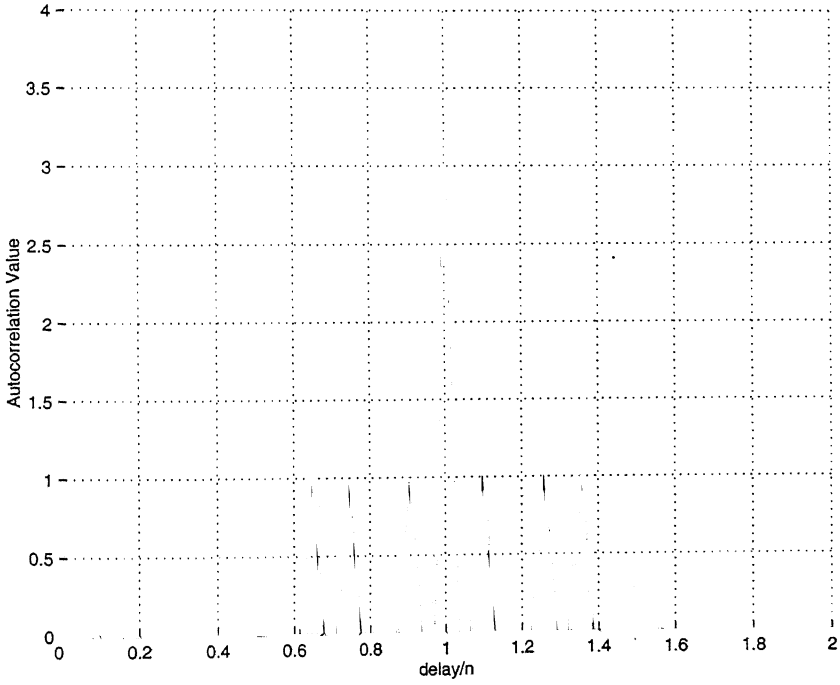

Figure 4.3.6: Autocorrelation of codeword C_3 of a (31,3,1,1) OOC based on Skolem Sequences

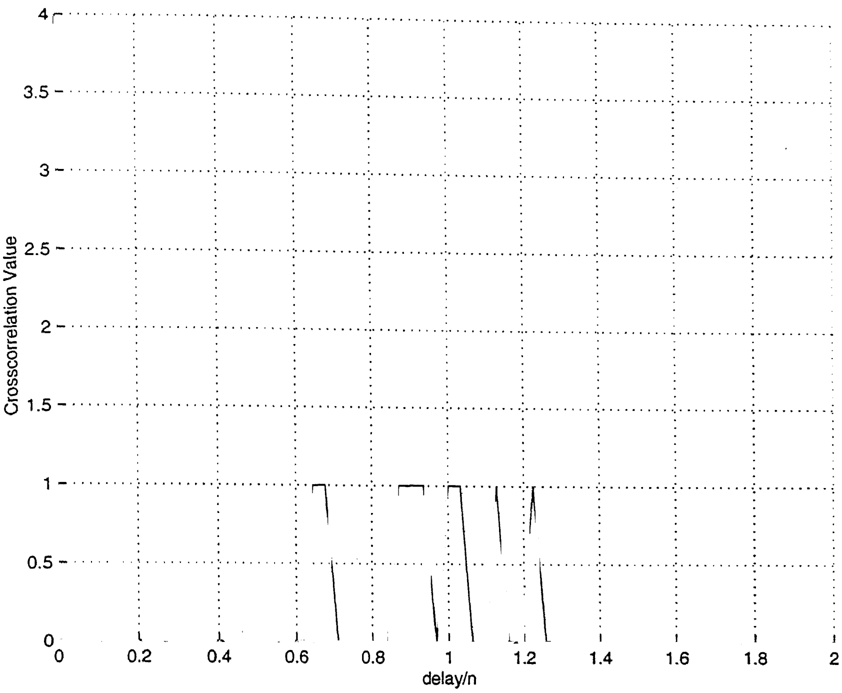

Figure 4.3.7: Crosscorrelation between codeword C_1 and codeword C_3 of a (31,3,1,1) OOC based on Skolem Sequences

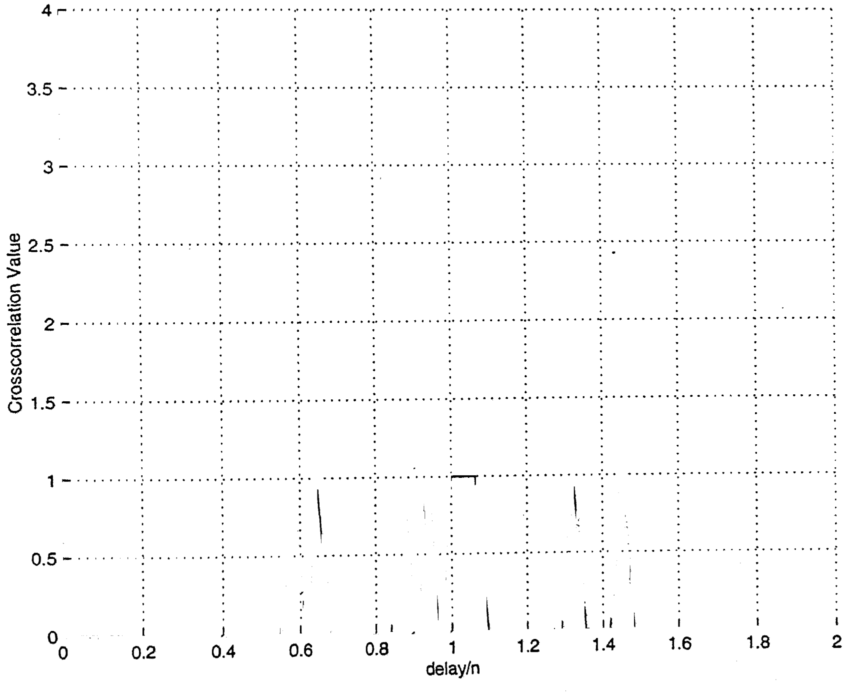

Figure 4.3.8: Crosscorrelation between codeword C_2 and codeword C_4 of a (31,3,1,1) OOC based on Skolem Sequences

6. The i^{th} codeword, therefore, is $\{0, i, x_{i(3,1)}\}$, where $x_{i(3,1)} = x_{i3} - x_{i1}$.

7. Write down the Skolem sequences of order M. Obtain $x_{i(3,1)}$ from the sequences for corresponding $i + M$, by adding M to all pairs of Skolem sequences.

8. Write down the resultant 3-sets and their corresponding codewords.

4.5 Discussion

A class of Optical Orthogonal Codes using Skolem Sequences has been presented in this chapter. The codewords of weight 3 are derived from appropriately translated Skolem sequences. A Generalized construction procedure for this class of OOCs is presented in section 4.4.

The construction technique has been illustrated with the help of two examples and the resultant codewords have been listed. The autocorrelation and crosscorrelation plots for the two examples have been shown. The plots show that the proposed codes have a maximum off-peak autocorrelation value of 1 for any codeword. Also, the maximum crosscorrelation value between any two codewords is equal to 1.

This class of codes have the following properties:

- The length of the codewords, $n = 6M + 1$
- The weight of the codeword, $w = 3$
- The maximum value of off-peak autocorrelation, $\lambda_a = 1$
- The maximum value of crosscorrelation, $\lambda_c = 1$
- The number of codewords $= M$

In Chapter 6, we present a comparison of the codes discussed in this chapter with the codes proposed in chapters 3 and 5, and also with various Optical Orthogonal Codes suggested earlier in the literature.

Chapter 5

Optical Orthogonal Codes based on Number Theory and Quadratic Residues

In this chapter, we present methods of constructing three different classes of Optical Orthogonal Codes. First, we discuss a technique for construction of OOCs using the Table of Primes. Next, we present construction of OOCs through partitioning of $GF(n)$, where n is the length of the codewords. Lastly, we construct OOCs using Quadratic Residues.

The first and the third class of codes presented in this chapter are variants of Prime Sequence codes [36] and Quadratic Congruence codes [46], respectively. We mention the properties of these classes of OOCs, and give examples of codewords.

5.1 OOCs based on Table of Primes

Definition 5.1.1 A number α is a primitive root[1] for prime p if $\alpha^x \not\equiv 1(mod\ \ p)$ for any $1 \leq x \leq p-1$.

For a code of length $p^2 - p$ and weight w, we take a prime number p and generate the complete elements of the $GF(p)$, using the primitive root α. Then we write

[1] A brief table of the primes and their primitive roots is given in Appendix D.

Table 5.1.1: Elements of $GF(5)$ modulo 5, Primitive root = 2

Elements	Equivalent
2^0	1
2^1	2
2^2	4
2^3	3

$(p-1)$ nonzero elements of $GF(p)$ in a sequence form, similar to the way the prime sequences are written. The $(p-1)$ different sequences, corresponding to $(p-1)$ different codewords are obtained by multiplying the original sequence by elements from $\{1, 2, \ldots, p-1\}$, respectively. Then by time-mapping these sequences into bit positions, we obtain the codewords.

We illustrate the concept with the help of an example.

Example 5.1.1: OOCs USING TABLE OF PRIMES FOR $p = 5$ AND $\alpha = 2$

For this we have elements of the field given in Table 5.1.1.

The $(p-1)$ nonzero elements of $GF(p)$, in this case, are represented by

$$S_1^5 = \{1 \ \ 2 \ \ 4 \ \ 3\}$$

As in the Prime Sequence codes, these values are thén time-mapped into corresponding bit positions in the code sequence, with the frame-length equal to p which is equal to 5 in this case. This means that each element of the field represents the location of a 1 in the frame of length p. There are a total of $(p-1)$ frames in the codeword, corresponding to $(p-1)$ nonzero elements of $GF(p)$.

Hence, the codeword corresponding to the above sequence is:

$C_1^5 = \{1 \ \ 2+p \ \ 4+2p \ \ 3+3p\}$

which is equivalent to, in the form of a w-set:

$C_1^5 = \{1 \ \ 7 \ \ 14 \ \ 18\}$

or, in terms of an actual code sequence (in 0's and 1's), it looks like

$C_1^5 = \{01000\ \ 00100\ \ 00001\ \ 00010\}$

We can generate $(p-1)$ codewords by multiplying the nonzero elements of $GF(p)$ by $\{1, 2, \ldots, p-1\}$, as

$S_1^5 = \{1\ \ 2\ \ 4\ \ 3\}$

$S_2^5 = \{2\ \ 4\ \ 3\ \ 1\}$

$S_3^5 = \{3\ \ 1\ \ 2\ \ 4\}$

$S_4^5 = \{4\ \ 3\ \ 1\ \ 2\}$

and the corresponding codewords then are:

$C_1^5 = \{01000\ \ 00100\ \ 00001\ \ 00010\}$

$C_2^5 = \{00100\ \ 00001\ \ 00010\ \ 01000\}$

$C_3^5 = \{00010\ \ 01000\ \ 00100\ \ 00001\}$

$C_4^5 = \{00001\ \ 00010\ \ 01000\ \ 00100\}$

The autocorrelation of codewords C_1 and C_3 of example 5.1.1 is shown in Fig. 5.1.1 and Fig. 5.1.2, respectively. As can be seen from Figs. 5.1.1 and 5.1.2, the peak value of autocorrelation is equal to the weight of the code (which is 4 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) in all the plots is equal to 1. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_1 and C_3 of example 5.1.1 is shown in Fig. 5.1.3. The crosscorrelation between codewords C_2 and C_4 is shown in Fig. 5.1.4. As can be seen from Figs. 5.1.3 and 5.1.4, the maximum crosscorrelation value between any two codewords is equal to $(p-2)$, which is 3 in this example.

5.1.1 Properties of OOCs using Table of Primes

The codewords generated using the Table of Primes have the following properties:

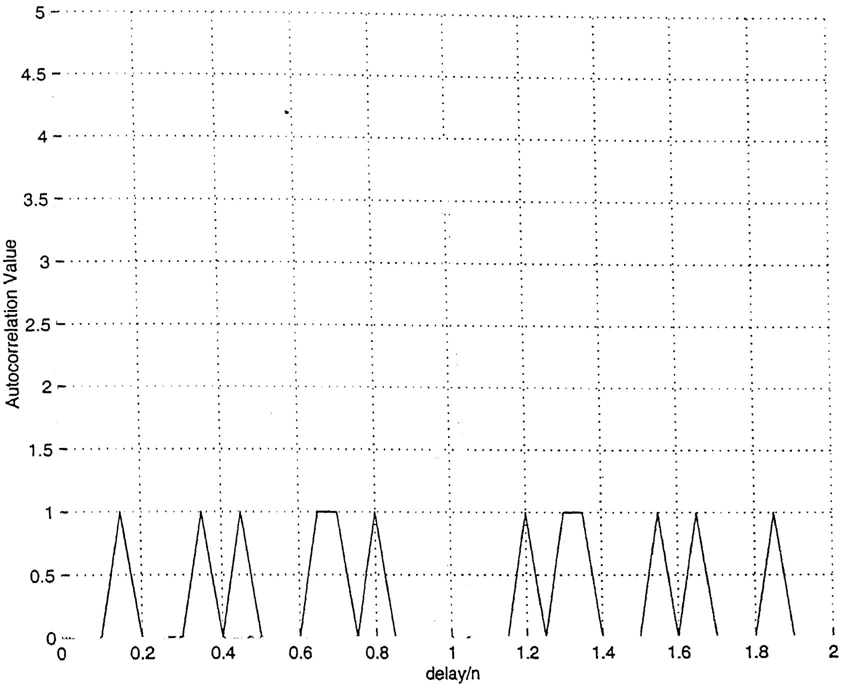

Figure 5.1.1: Autocorrelation of codeword C_1 of a (20,4,1,3) OOC based on Table of Primes

- The length of the codewords, $n = p^2 - p$
- The weight of the codewords, $w = p - 1$
- The maximum value of off-peak autocorrelation, $\lambda_a = 1$
- The maximum value of crosscorrelation, $\lambda_c = p - 2$
- The number of codewords, $M = p - 1$

5.2 OOCs based on Number Theory

Here we present a method of construction of $(n, 3, 2, 2)$ code using the concepts of number theory. The number of codewords, t, of this $(n, 3, 2, 2)$ code are generated by partitioning $GF(n)$ into t 3-sets, where $n = 3t + 2$ and n is a prime number such that 3 should be a primitive root of n. The method of construction is as follows: using the

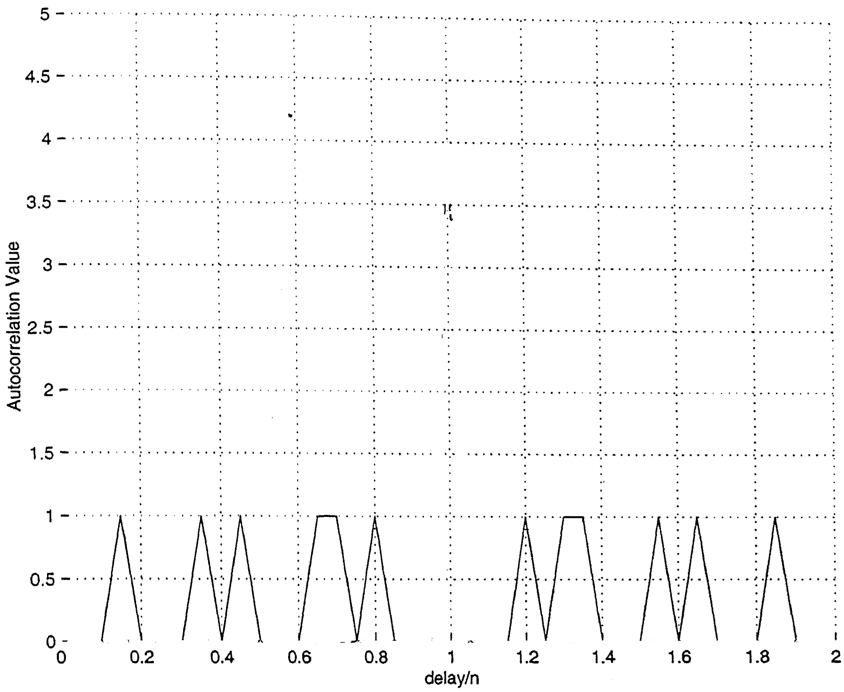

Figure 5.1.1: Autocorrelation of codeword C_1 of a (20,4,1,3) OOC based on Table of Primes

- The length of the codewords, $n = p^2 - p$
- The weight of the codewords, $w = p - 1$
- The maximum value of off-peak autocorrelation, $\lambda_a = 1$
- The maximum value of crosscorrelation, $\lambda_c = p - 2$
- The number of codewords, $M = p - 1$

5.2 OOCs based on Number Theory

Here we present a method of construction of $(n, 3, 2, 2)$ code using the concepts of number theory. The number of codewords, t, of this $(n, 3, 2, 2)$ code are generated by partitioning $GF(n)$ into t 3-sets, where $n = 3t + 2$ and n is a prime number such that 3 should be a primitive root of n. The method of construction is as follows: using the

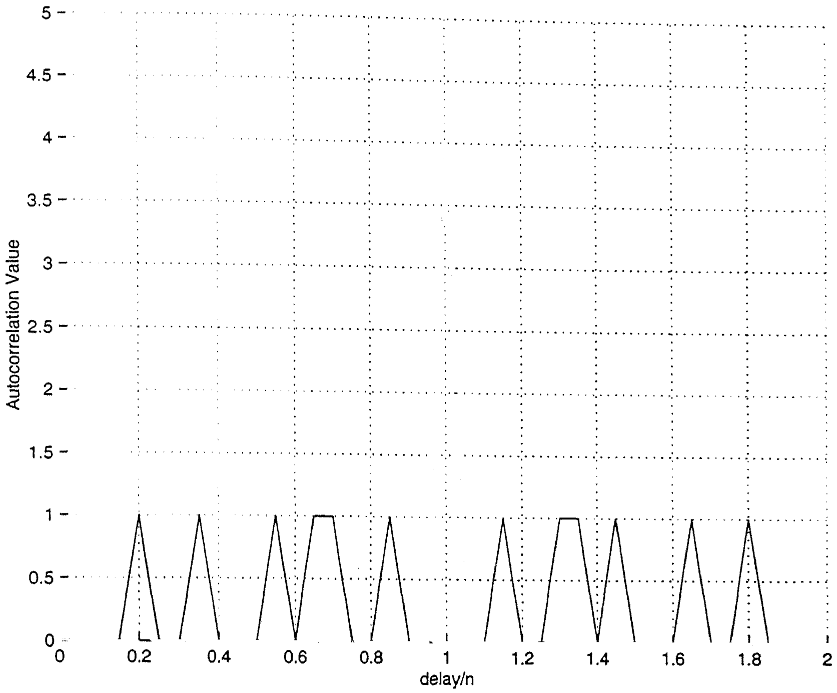

Figure 5.1.2: Autocorrelation of codeword C_3 of a (20,4,1,3) OOC based on Table of Primes

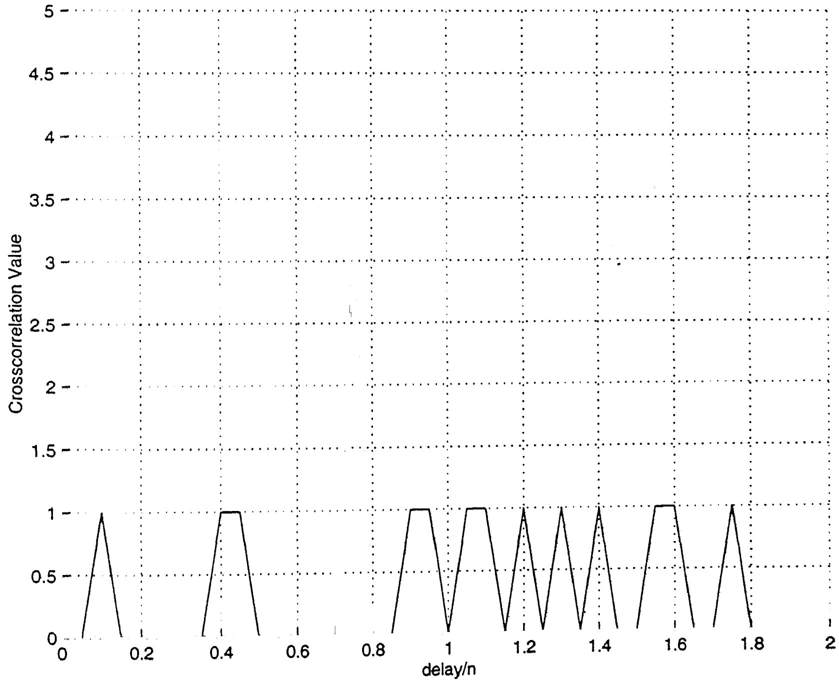

Figure 5.1.3: Crosscorrelation between codeword C_1 and codeword C_3 of a (20,4,1,3) OOC based on Table of Primes

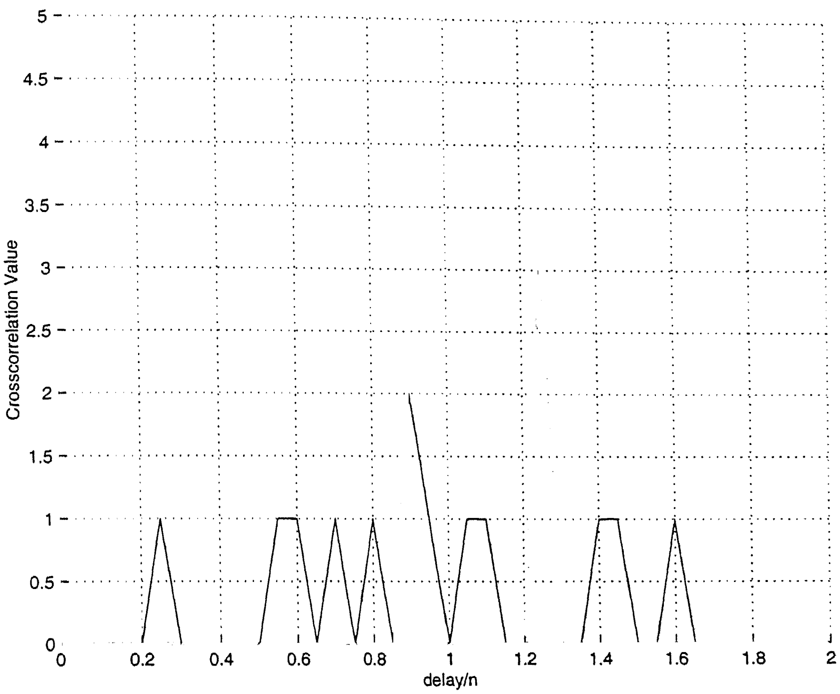

Figure 5.1.4: Crosscorrelation between codeword C_2 and codeword C_4 of a (20,4,1,3) OOC based on Table of Primes

prime number n and its primitive root α, generate the elements of the fields α^i. Now the i^{th} codeword out of t possible codewords can be written in the form of a w-set as per the following equation:

$$\{1, \ \alpha^{w+(i-1)}, \ \alpha^{2w+d+(i-1)}\}, \text{ where } d = \lambda_c. \tag{5.2.1}$$

Example 5.2.1: OOCs using Number Theory for $n = 17$ and $\alpha = 3$

For this we have elements of the field given in Table 5.2.1. Here $\alpha = 3$, primitive root of $GF(n)$, and $n = 17$.

In this case, we have 5 different codewords given by

$\{1, \ \alpha^3, \ \alpha^8\} \Rightarrow \{1, \ 10, \ 16\}$

$\{1, \ \alpha^4, \ \alpha^9\} \Rightarrow \{1, \ 13, \ 14\}$

$\{1, \ \alpha^5, \ \alpha^{10}\} \Rightarrow \{1, \ 5, \ 8\}$

$\{1, \ \alpha^6, \ \alpha^{11}\} \Rightarrow \{1, \ 15, \ 7\}$

Table 5.2.1: Elements of $GF(17)$ modulo 17, Primitive root = 3

Elements	Equivalent
3^0	1
3^1	3
3^2	9
3^3	10
3^4	13
3^5	5
3^6	15
3^7	11
3^8	16
3^9	14
3^{10}	8
3^{11}	7
3^{12}	4
3^{13}	12
3^{14}	2
3^{15}	6

$\{1, \ \alpha^7, \ \alpha^{12}\} \Rightarrow \{1, \ 11, \ 4\}$

The corresponding codewords are:

$C_1 = \{0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\}$

$C_2 = \{0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\}$

$C_3 = \{0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\}$

$C_4 = \{0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\}$

$C_5 = \{0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\}$

The autocorrelation of codewords C_3 and C_5 of example 5.2.1 is shown in Fig. 5.2.1 and Fig. 5.2.2, respectively. As can be seen from Figs. 5.2.1 and 5.2.2, the peak value of autocorrelation is equal to the weight of the code (which is 3 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) in all the plots never exceeds 2.

The crosscorrelation between codewords C_1 and C_4 of example 5.2.1 is shown

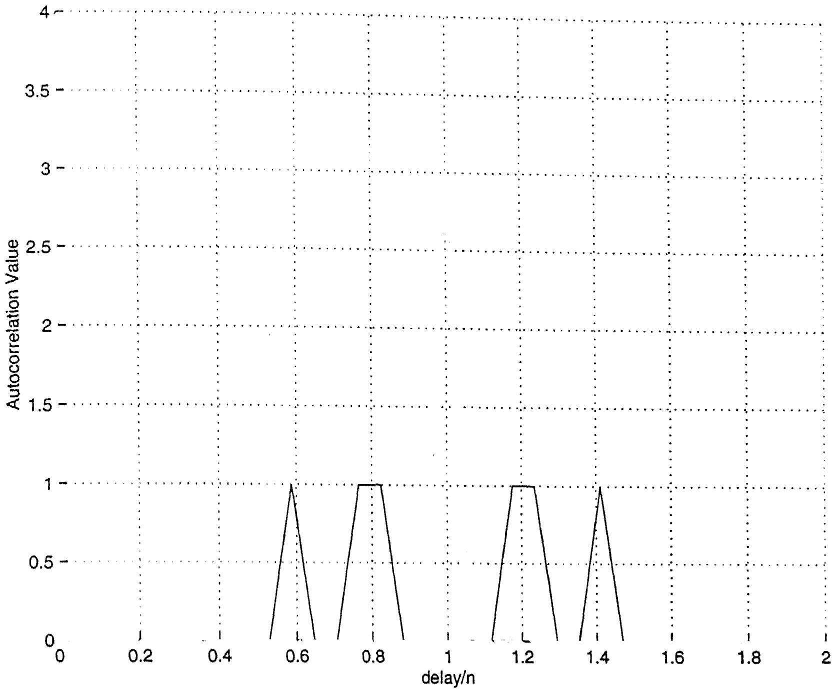

Figure 5.2.1: Autocorrelation of codeword C_3 of a (17,3,2,2) OOC based on Number Theory

in Fig. 5.2.3. The crosscorrelation between codewords C_3 and C_5 is shown in Fig. 5.2.4. As can be seen from Figs. 5.2.3 and 5.2.4, the maximum crosscorrelation value between any two codewords never exceeds 2.

5.2.1 Properties of OOCs using Number Theory

The codewords generated using the Number Theory approach have the following properties:

- The number of codewords, $M = t$
- The weight of the codeword, $w = 3$, 3 should be a primitive root of n.
- The length of the codeword, $n = 3t + 2$, n is a prime. Though we have 3 as primitive root of many primes such as 7, 17, 31, 43 *etc.*, but not many of these primes satisfy the requirement $n = 3t + 2$. The smallest number satisfying the requirement is 17.

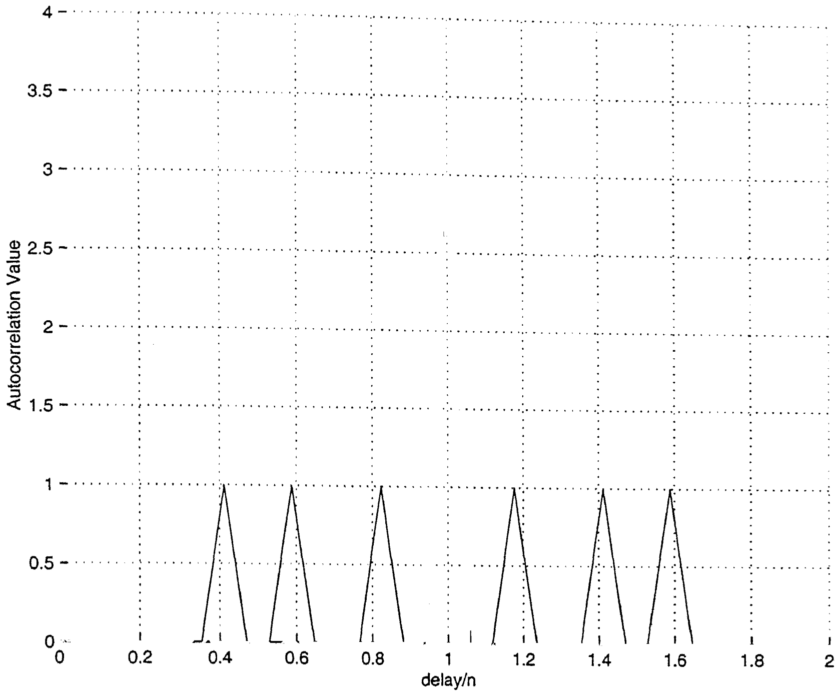

Figure 5.2.2: Autocorrelation of codeword C_5 of a (17,3,2,2) OOC based on Number Theory

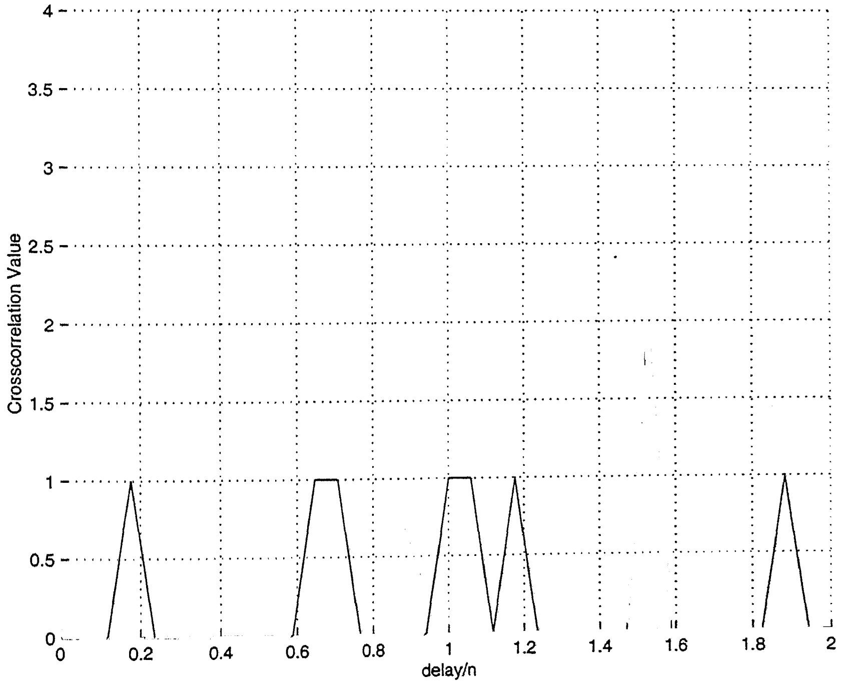

Figure 5.2.3: Crosscorrelation between codeword C_1 and codeword C_4 of a (17,3,2,2) OOC based on Number Theory

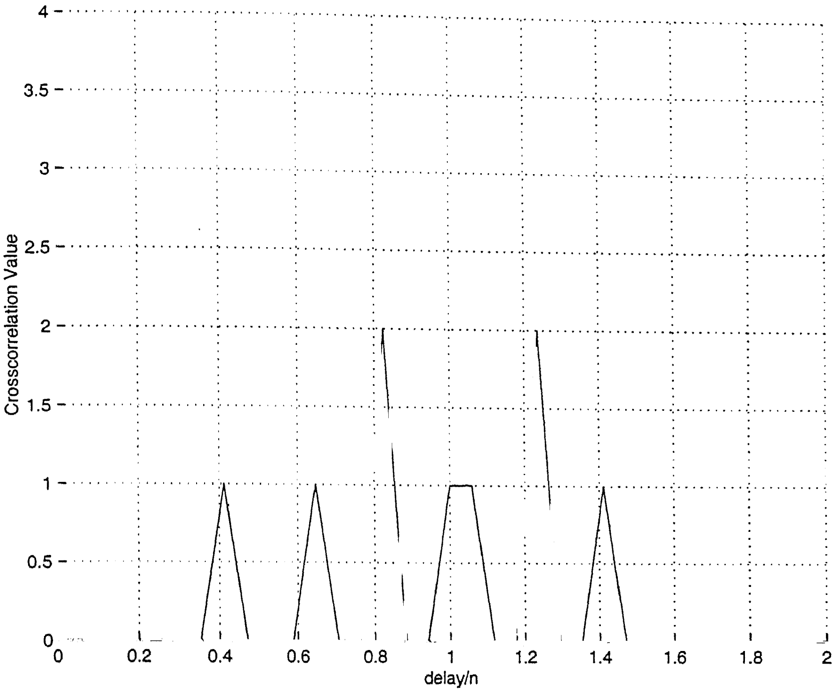

Figure 5.2.4: Crosscorrelation between codeword C_3 and codeword C_5 of a (17,3,2,2) OOC based on Number Theory

- The maximum value of off-peak autocorrelation, $\lambda_a = 2$

- The maximum value of crosscorrelation, $\lambda_c = 2$

5.3 Optical Orthogonal Codes based on Quadratic Residues

In this section, we present the construction of Optical Orthogonal Codes using Quadratic Residues. These codes appear similar to those obtained using Quadratic Congruences [46], but, are different as discussed later.

Definition 5.3.1 For any prime p, a is a *quadratic residue* mod p if $x^2 \equiv a \pmod{p}$ for any integer x.

For any prime p, there are as many quadratic residues (QR) as there are quadratic non-residues. For example, when $p = 11$, the QRs are {0,1,3,4,5,9}.

5.3.1 Construction of Codes

Optical Orthogonal Codes can be constructed using Quadratic Residues (QR) using the following steps:

1. For any prime p, let the quadratic residues be $X = \{0, x_1, x_2, \ldots, x_{(p-1)/2}\}$.

There is a total of $(p-1)/2$ quadratic residues. 0 is a quadratic residue (QR) as well as a quadratic non-residue.

2. Write the QR sequence as $QR = \{q_1, q_2, \ldots, q_p\}$, where $q_1 = q_p = 0$, $q_2 = x_1$, $q_3 = x_2$ and so on, and $q_k = q_{p-k+1}$ for $1 \leq k \leq p$. This forms the first QR sequence, denoted by Q_1.

3. The j^{th} QR sequence, $j \in \{1, 2, \ldots, p-1\}$, can be generated using Q_1 by multiplying each element of Q_1 by j (modulo p).

4. Translate these QR sequences into $(p-1)$ codewords by time-mapping the bit positions.

Example 5.3.1: OOCs USING QUADRATIC RESIDUES

Let us take a prime number, $p = 5$. The QRs for this are $\{0, 1, 4\}$. The number of QR sequences is equal to, $p - 1 = 4$.

The first QR sequence, Q_1, is {0,1,4,1,0}. The remaining QR sequences, Q_2, Q_3 and Q_4, obtained using Step 3, are:

$Q_2 = \{0,2,3,2,0\}$

$Q_3 = \{0,3,2,3,0\}$

$Q_4 = \{0,4,1,4,0\}$

The corresponding codewords are:

$C_1 = \{10000 \quad 01000 \quad 00001 \quad 01000 \quad 10000\}$

$C_2 = \{10000 \quad 00100 \quad 00010 \quad 00100 \quad 10000\}$

$C_3 = \{10000 \quad 00010 \quad 00100 \quad 00010 \quad 10000\}$

$C_4 = \{10000 \quad 00001 \quad 01000 \quad 00001 \quad 10000\}$

The length of each of these codewords is 25. In terms of w-sets, these codewords can be represented (modulo 25) as shown below.

$C_1 = \{0,6,14,16,20\}$

$C_2 = \{0,7,13,17,20\}$

$C_3 = \{0,8,12,18,20\}$

$C_4 = \{0,9,11,19,20\}$

The autocorrelation of codewords C_1 and C_3 of example 5.3.1 is shown in Fig. 5.3.1 and Fig. 5.3.2, respectively. As can be seen from Figs. 5.3.1 and 5.3.2, the peak value of autocorrelation is equal to the weight of the code (which is 5 in this example) and it occurs at a normalized delay of 1. The maximum off-peak autocorrelation value (side-lobe) in all the plots never exceeds 2. The plots differ for different codewords because the distribution of 1's in them is different.

The crosscorrelation between codewords C_1 and C_3 of example 5.3.1 is shown in Fig. 5.3.3. The crosscorrelation between codewords C_2 and C_4 is shown in Fig. 5.3.4. As can be seen from Figs. 5.3.3 and 5.3.4, the maximum crosscorrelation value between any two codewords never exceeds 2.

5.3.2 Properties of OOCs using Quadratic Residues

As mentioned ealier, these codes appear similar to those obtained using Quadratic Congruences [46] but are different in their correlation properties. While the OOCs based on Quadratic Congruences have a very high maximum value of crosscorrelation between any two codewords, λ_c= 4, and the maximum off-peak autocorrelation value, λ_a= 2, the OOCs proposed in this section using Quadratic Residues have a maximum value of crosscorrelation between any two codewords, λ_c= 2 while having all other code parameters the same as that in Quadratic Congruence codes.

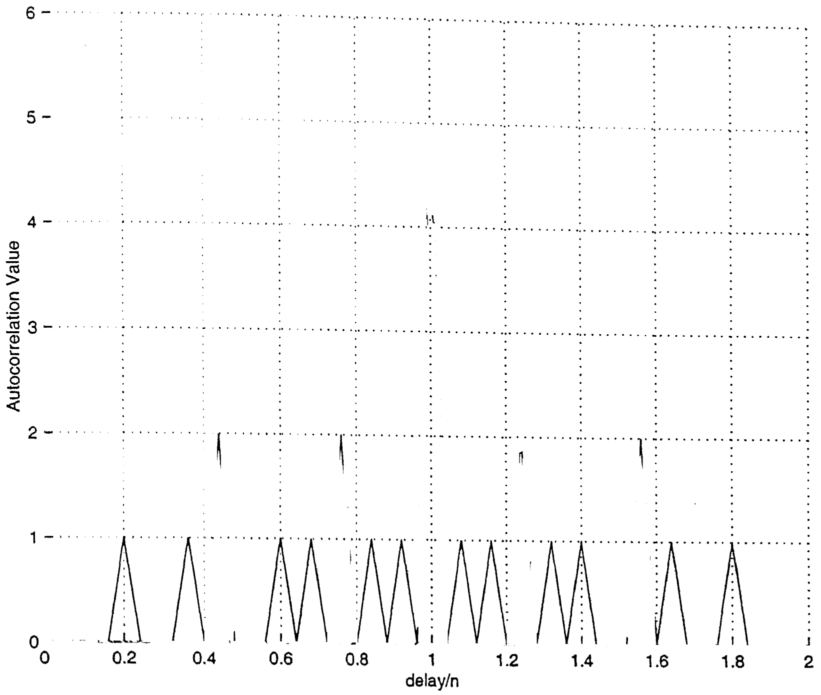

Figure 5.3.1: Autocorrelation of codeword C_1 of a (25,5,2,2) OOC based on Quadratic Residues

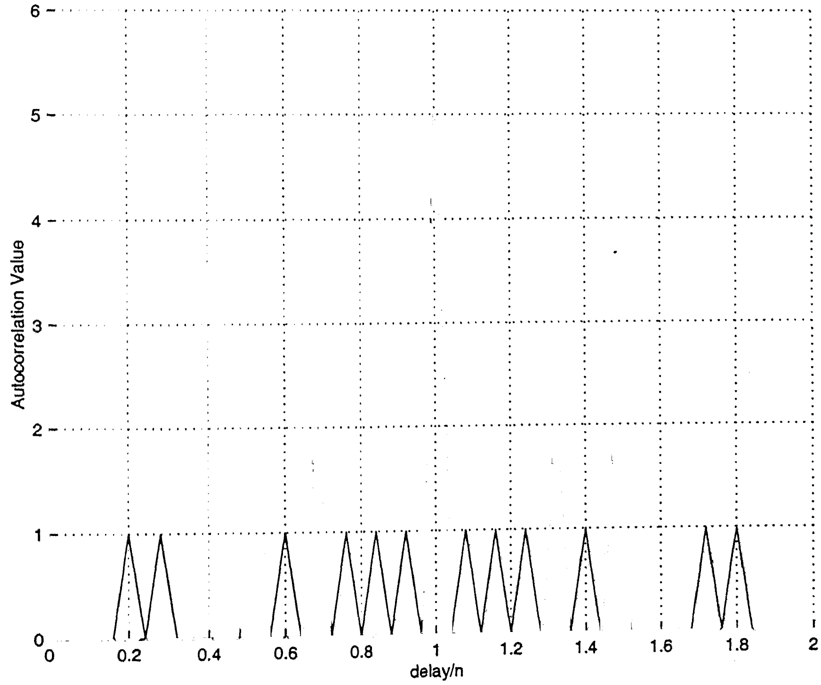

Figure 5.3.2: Autocorrelation of codeword C_3 of a (25,5,2,2) OOC based on Quadratic Residues

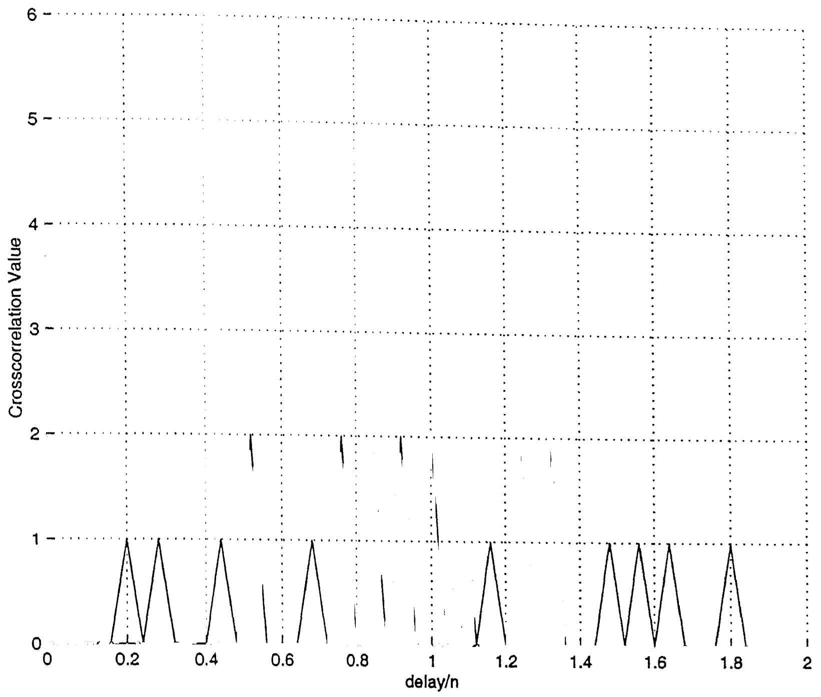

Figure 5.3.3: Crosscorrelation between codeword C_1 and codeword C_3 of a (25,5,2,2) OOC based on Quadratic Residues

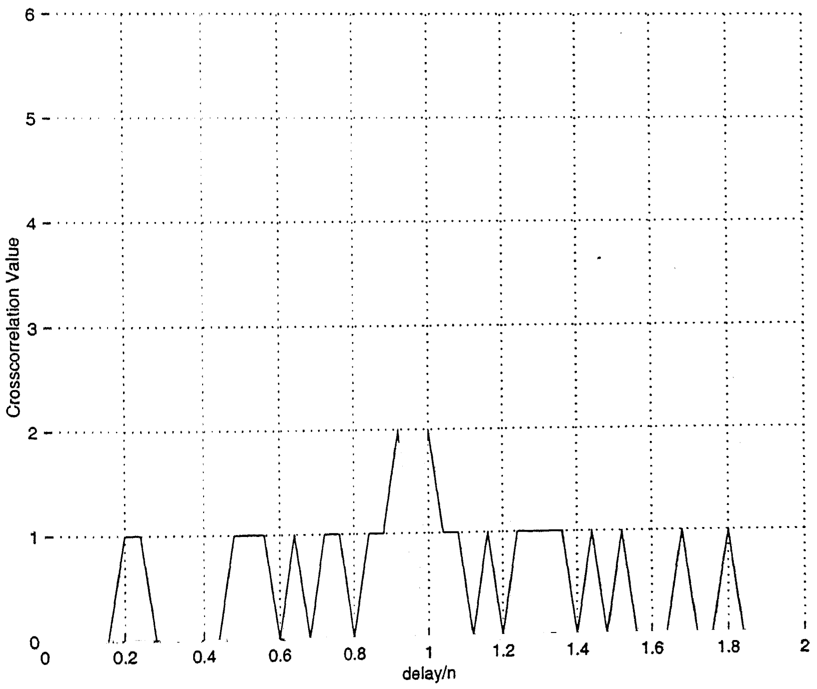

Figure 5.3.4: Crosscorrelation between codeword C_2 and codeword C_4 of a (25,5,2,2) OOC based on Quadratic Residues

The codewords have the following properties:

- The length of the codeword, $n = p^2 = 25$
- The weight of the codeword, $w = p = 5$
- The maximum value of off-peak autocorrelation, $\lambda_a = 2$
- The maximum value of crosscorrelation, $\lambda_c = 2$
- The number of codewords, $M = p - 1$

5.4 Discussion

Three different classes of Optical Orthogonal Codes have been introduced in this chapter.

The first class of OOCs presented in this chapter are constructed using the Table of Primes and can be generated for any prime number. These codes are variants of Prime Sequence codes [36]. The OOCs developed are $(p^2 - p, p - 1, 1, p - 2)$, and each code has $p - 1$ codewords. An illustrative example for construction of codewords using this method has been given. The codewords have poorer crosscorrelation but better off-peak autocorrelation than the OOCs using Prime Sequences.

The next class of OOCs presented in this chapter is constructed using the Number Theory approach by partitioning $GF(n)$ into t 3-sets, where n and t are the length of codewords and the number of codewords, respectively. Each codeword has a weight, $w = 3$. These codes can be generated for any prime number n, where $n = 3t + 2$, and 3 should be a primitive root of n. The OOCs are $(n, 3, 2, 2)$. An illustrative example for construction of codewords using this method has been given for $n = 17$.

Lastly, we proposed a method for construction of OOCs using Quadratic Residues. These codes appear similar to those obtained using Quadratic Congruences [46], but, are different in their crosscorrelation properties. While the OOCs based on Quadratic Congruences have a very high maximum value of crosscorrelation (equal to 4) between any two codewords, the OOCs constructed using Quadratic Residues have a maximum value of crosscorrelation between any two codewords of only 2. All the other code parameters are same as that of Quadratic Congruence codes. We included an example for generation of codewords using this approach. This class of OOCs can be generated for any prime number, and the resultant codes are $(p^2, p, 2, 2)$.

In Chapter 6, we present a brief comparison of the codes proposed in this thesis with various Optical Orthogonal Codes suggested earlier in the literature.

Chapter 6

Discussion

In this chapter, we present a comparison of the Optical Orthogonal Codes proposed in Chapters 3-5, and those reviewed in Chapter 2.

We have compared the OOCs using two criteria. First, we compare the optimality of construction techniques for the OOCs by findng out the number of codewords actually available, compared to the number of codewords theoretically possible for given code parameters. This can be used as one basis for commenting on the effectiveness of the construction technique. For this purpose, we calculate the maximum number of codewords for each class of OOCs. The minimum length required to generate a given number of codewords can also be obtained from the upper bounds for a specific set of code parameters.

Then, the multiple access interference rejection capability of the various OOCs is briefly discussed. The maximum values of correlation constraint is suggestive of how worse the system can perform. For the discussion, we consider the fact that the channel is a "Z" channel, meaning that errors result only when a "1" is decided at the receiver, when actually a "0" was transmitted. We consider the multiple user interference as the dominant source of noise. The maximum number of simultaneous users can be decided by the distribution of interference.

Our discussion and comparison is on the basis of interference patterns. A detailed discussion on the performance of optical CDMA systems is given in [74–77]. Other noise sources such as APD noise and thermal noise have been considered in [78–81]. The effects of characteristics of multimode optical fiber channel on the performance of FO-CDMA communications has been theoretically analysed by Walker [82, 83]. The effects of laser phase drift for coherent optical CDMA are discussed in [84]. The effects of optical amplifier and photodetector noise on the performance of Optical CDMA systems have been discussed by Ormondroyd et. al. [85].

6.1 Number of Codewords in an OOC

In this section, we discuss the upper bounds on the number of codewords in an OOC, and how the OOCs discussed in this thesis approach them.

The number of codewords in an OOC is denoted by M. The cyclic shift of a codeword is not considered as another codeword. The largest possible size of an $(n, w, \lambda_a, \lambda_c)$ code is denoted by $\Phi(n, w, \lambda_a, \lambda_c)$. A code that achieves the maximum possible size, $M = \Phi(n, w, \lambda_a, \lambda_c)$, is said to be an *optimal* code. This optimality is in terms of the number of codewords that are available for a given set of code parameters and is not meant for evaluating the performance criterion of practical systems.

The Johnson bound for the largest possible value of $M = \Phi(n, w, \lambda_a, \lambda_c)$ is given as [32]

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{(n-1)(n-2)\ldots(n-\lambda)}{w(w-1)(w-2)\ldots(w-\lambda)} \right\rfloor, \tag{6.1.1}$$

where $\lambda = max(\lambda_a, \lambda_c)$.

This bound is particularly applicable for small values of λ. For larger values of $\lambda(\geq 6)$, a suitable bound can be found in [31].

When $\lambda_a = \lambda_c = 1$, the above bound has been modified to the forms [32]:

$$\Phi(n, w, 1, 1) \leq \left\lfloor \frac{(n-1)}{w(w-1)} \right\rfloor \quad \text{for } n \equiv 1 \mod 2 \tag{6.1.2}$$

$$\Phi(n, w, 1, 1) \leq \left\lfloor \frac{(n-2)}{w(w-1)} \right\rfloor \quad \text{for } n \equiv 0 \mod 2 \tag{6.1.3}$$

Using equation 6.1.2, for optimal codes, i.e., when $M = \Phi(n, w, \lambda_a, \lambda_c)$, we have a minimum length of the codewords of the $(n, w, 1, 1)$ code, $n \geq Mw(w-1) + 1$.

Yang et. al. [66] have considered the Johnson bound of equation 6.1.1 for the condition when $\lambda_a \neq \lambda_c$ and suggested a modified bound for $(n, w, \lambda + m, \lambda)$ codes. This bound is stronger than the bound in equation 6.1.1 and is given as

$$\Phi(n, w, \lambda + m, \lambda) \leq \left\lfloor \frac{(n-1)(n-2)\ldots(n-\lambda)(\lambda+m)}{w(w-1)(w-2)\ldots(w-\lambda)} \right\rfloor \tag{6.1.4}$$

For instance, considering $(n, w, 2, 1)$ OOCs, the bound in equation 6.1.4 is tighter than the Johnson bound of equation 6.1.1 for $(n, w, 2, 2)$ codes provided $n > 2w - 2$. Equation 6.1.4 is only a generalization of equation 6.1.1 for $\lambda = 1$. For $\lambda \geq 2$, the bound on $(n, w, 2, 2)$ obtained by setting $m = 0$ in equation 6.1.4 is weaker than the bound in equation 6.1.1.

We now consider the OOCs one at a time, and compare them against the upper bounds on the number of codewords in the OOC.

1. OOCs based on Prime Sequences: First we consider the OOCs based on Prime Sequences, discussed earlier in section 2.1 and example 2.1.1. Equation 6.1.1 gives the maximum possible number of codewords as

$$\Phi(25, 5, 4, 2) \leq \left\lfloor \tfrac{24.23.22.21}{5.4.3.2.1} \right\rfloor = 2125$$

Since $\lambda_a \neq \lambda_c$ in this case, we use equation 6.1.4 to get a stronger upper bound on the maximum number of codewords as

$$\Phi(25, 5, 4, 2) \leq \left\lfloor \tfrac{24.23.4}{5.4.3} \right\rfloor = 36$$

However, the number of codewords in the OOC that are obtained from the prime sequences is only 5. This is much lower than what can theoretically be obtained from the given code parameters, as shown above.

In fact, as the length of the OOCs based on the Prime Sequences increases, the number of codewords obtained become far less compared to the maximum possible number that could be obtained using the code parameters.

2. OOCs based on Quadratic Congruences: For the OOCs based on Quadratic Congruences discussed in section 2.3, and example 2.3.1, we get the maximum possible number of codewords from equation 6.1.1 as

$$\Phi(25,5,2,4) \leq \left\lfloor \frac{24.23.22.21}{5.4.3.2.1} \right\rfloor = 2125$$

But the number of codewords we obtain is only 4. This shows that for the code parameters used in the construction of OOCs using Quadratic Congruences, the number of codewords is very small.

As in the case of the OOCs based on the Prime Sequences, an increase in the length of codewords does not give a corresponding increase in the number of codewords. The number of codewords obtained are far less compared to the maximum possible number that could be theoretically obtained using the code parameters.

3. OOCs based on Projective Geometry: In example 2.4.1, the number of codewords obtained is equal to the maximum possible number of codewords, which is equal to 1, in the example.

$$\Phi(7,3,1,1) \leq \left\lfloor \frac{6}{3.2} \right\rfloor = 1 = M$$

This, therefore, is a trivial example of an optimal code.

In general, for any $PG(m,q)$ code, with $s = 1$, we can have constructions for $\lambda_a = \lambda_c = \lambda = 1$. The number of maximum possible codewords using equation 6.1.1 is

$$\Phi(n, w, 1, 1) \leq \left\lfloor \frac{q^{m+1}-q}{q(q^2-1)} \right\rfloor = \left\lfloor \frac{q^m-1}{q^2-1} \right\rfloor ,$$

which is an integer equal to $\frac{q^m-1}{q^2-1}$, if and only if, m is even. We can obtain optimal codes for these specific values in $PG(m, q)$.

However, for higher values of λ, the codes are not optimal, e.g., in example 2.4.1.1, we have only 4 codewords against a maximum possible number of codewords of 29.

4. **OOCs based on Error correcting codes:** In this method, we obtain codewords from constant weight error correcting codes having a minimum distance between them of $d \geq 2(w - \lambda)$. A large number of codes that satisfy this constraint with equality give us optimal codes.

In example 2.7.1, the OOC is $(19, 3, 1, 1)$, and is obtained by a constant weight error correcting code having a length 19, weight 3, and a minimum distance between any two codewords as 4. The number of codewords in this OOC is 3. Using equation 6.1.1, we verify that this is the maximum number of codewords that can be obtained using these parameters:

$$\Phi(19, 3, 1, 1) \leq \left\lfloor \frac{18}{3.2} \right\rfloor = 3$$

Similarly the code shown in example 2.7.2 is also an optimal code.

Now, we consider the case when $\lambda_a = \lambda_c = 2$. The number of maximum possible codewords using equation 6.1.1, for the code of example 2.7.3, is

$$\Phi(18, 4, 2, 2) \leq \left\lfloor \frac{17.16}{4.3.2} \right\rfloor = 11,$$

which is equal to the number of codewords actually generated in example 2.7.3.

5. **OOCs based on Hadamard matrices:** In this method, we obtain codewords of OOCs from a truncation of Hadamard matrices. Here we check for the maximum number of codewords that can be generated for the given parameters.

In example 3.3.1, we have a (7,3,1,2) OOC with two usable codewords, as against a maximum possible 5 codewords:

$$\Phi(7,3,1.2) \leq \left\lfloor \frac{6.5}{3.2.1} \right\rfloor = 5$$

In example 3.3.2, the OOC is $(15,7,3,4)$ and has nine codewords. Using equation 6.1.1, we have the maximum number of codewords:

$$\Phi(15,7,3,4) \leq \left\lfloor \frac{14.13.12.11}{7.6.5.4.3} \right\rfloor = 9$$

In fact, the number of codewords that can be constructed using this approach is near optimal, as the length of the codewords is increased. Furthermore, these codewords have a very small length.

6. **OOCs based on Skolem Sequences:** The Skolem sequences give us a method of choosing two integers uniquely from the set $\{1, 2, \ldots, 2M\}$ such that the differences between any two integers are unique and form the set $\{1, 2, \ldots, M\}$. We have proposed a construction procedure based on a translated version of these sequences for OOCs having M codewords with $\lambda_a = \lambda_c = \lambda = 1$. The codes are of the form $(6M+1, 3, 1, 1)$, where $M \equiv 0 \pmod 4$ or $M \equiv 1 \pmod 4$.

Here we verify that these are optimal codes and that this class of OOCs require the minimum possible code length for the given code parameters.

In example 4.3.2.1, we have a (25,3,1,1) OOC based on Skolem Sequences, and this OOC has four usable codewords. The maximum possible number of codewords for these parameters is

$$\Phi(25,3,1,1) \leq \left\lfloor \frac{24}{3.2} \right\rfloor = 4$$

Therefore, the code constructed in example 4.3.2.1 is an optimal code.

Similarly, in example 4.3.2.2, we have a (31,3,1,1) OOC using Skolem Sequences with 5 codewords. Using equation 6.1.1, we can show again the maximum number of codewords for these parameters as

$$\Phi(31,3,1,1) \leq \left\lfloor \frac{30}{3.2} \right\rfloor = 5$$

Therefore, the OOC of example 4.3.2.2 is also optimal.

In fact, the OOCs that are constructed using this approach are always optimal, because $\Phi(6M+1,3,1,1)) \leq \lfloor \frac{6M}{3.2} \rfloor = M$. Furthermore, these codewords have a minimum possible length of $(6M+1)$, to generate M codewords, each with weight 3 and correlation constraints of 1.

7. OOCs based on Table of Primes: In Chapter 5 of the thesis, we presented a class of OOCs based on the Table of Primes. These are variants of OOCs based on the Prime Sequences. The codes are of the form $(p^2-p, p-1, 1, p-2)$, where p is a prime number.

In example 5.1.1, we have a (20,4,1,3) OOC based on the table of Primes and this OOC has four codewords. The maximum possible number of codewords for these parameters is

$$\Phi(20,4,1,3) \leq \left\lfloor \frac{19.18.17}{4.3.2.1} \right\rfloor = 484$$

Like the OOCs based on Prime sequences, these codes are also not optimal. Furthermore, as the length of the codewords increases, the number of codewords are far less compared to the maximum possible number of codewords for the given parameters.

8. OOCs based on Number Theory: This class of OOCs is obtained through the partitioning of $GF(n)$, where 3 is a primitive root of n, into t sets. The codes are of the form $(3t+2,3,2,2)$ and the number of codewords is t.

In example 5.2.1, where we have a (17,3,2,2) OOC based on the Number Theory approach, we obtain the maximum possible number of codewords as

$$\Phi(17,3,2,2) \leq \left\lfloor \frac{16.15}{3.2.1} \right\rfloor = 40$$

These codes are not optimal as the actual number of codewords (t) is only 5. However, the length of these codewords is smaller than (25,5,4,2) Prime Sequence codes.

9. OOCs based on Quadratic Residues: For the OOCs based on Quadratic Residues in example 5.3.1 and section 5.3, we get the maximum possible number of codewords from equation 6.1.1 as

$$\Phi(25,5,2,2) \leq \left\lfloor \frac{24.23}{5.4.3} \right\rfloor = 9$$

But the number of codewords we obtain is only 4. This shows that for the code parameters used in the construction of OOCs using Quadratic Residues, the number of codewords is relatively small. An increase in length of codewords does not result in an increase in the number of codewords in the same proportion.

6.1.1 Number of Codewords : A Comparison

The OOCs based on Prime Sequences and Quadratic Congruences, have a very small number of codewords compared to the maximum possible number of codewords given by the Johnson bound for a given set of code parameters. Therefore, in order to have a moderate number of codewords, these OOCs or their variants require either longer code lengths or a relaxation in the correlation constraints. The OOCs obtained from constant weight error correcting codes approach the Johnson bound. Some classes of optimal codes can also be constructed using the Projective Geometry approach for some specific values of code parameters.

The OOCs based on Hadamard matrices have smaller code lengths for a given number of codewords, compared to the OOCs using Prime Sequences and Quadratic Congruences. Another advantage of this code is that the codewords can be generated for any length n, for which a corresponding Hadamard matrix exists for order $(n+1)$. So we have a large set of code lengths to choose from, compared to the OOCs that are generated using a prime number, such as, Prime Sequences, Quadratic Congruences, and Projective Geometry, etc.

The OOCs proposed in Chapter 4, using Skolem sequences are the optimal codes for a given set of code parameters. The only restriction on the number of codewords is that this number has to be either 0 (mod 4) or 1 (mod 4). This class of OOCs has the minimum code length theoretically possible for a given number of the codewords.

The OOCs using the Table of Primes are, as in the case of Prime Sequences, not optimal. These codes are a variant of OOCs using Prime sequences. The OOCs using the number theory approach, as described in Chapter 5, require shorter lengths of codewords for $\lambda = 2$. The OOCs using the Quadratic Residues have the same number of codewords as in the case of codes using Quadratic Congruences. But these codes have a lower value of maximum crosscorrelation than the Quadratic Congruence codes, while keeping all the other parameters exactly the same.

As per the construction procedures described here, it is clear that the OOCs based upon the Skolem sequences appear to be the best. On the basis of our studies, we observe that the OOCs constructed using a prime number as their basis, such as, Prime Sequences, Quadratic Congruences, Quadratic Residues, etc., are not optimal from the point of view of their construction procedure vis-à-vis the Johnson bound.

6.2 Multiple Access Interference

In this section, we discuss some issues related with the performance of the OOCs in a multiple user scenario such as Fiber Optic CDMA system. We consider only those aspects of performance that directly result from the use of OOCs. The discussion is general in nature and may be applicable to other CDMA systems as well.

To begin with, we summarize the assumptions made in the following discussion.

1. An error occurs while transmitting data in a communication channel, if a transmitted data bit "0" is decoded in the receiver as a bit "1" and vice versa. This happens due to additive noise in the channel and other interference sources. In a FO-CDMA system, a "0" corresponds to no light and a "1" corresponds to maximum

light intensity (extinction ratio is assumed to be zero). As the optical systems are positive systems, an error occurs only if the desired receiver wrongly decides a "1" instead of a transmitted "0". However, when a "1" is transmitted, there will be no error because it cannot be converted to a "0"in any case. The data bits "0" and "1" are transmitted with an equal probability.

2. The multiple access interference (also called multiple user interference) is assumed to be the only source of noise. In practical systems, the multiple access interference is the dominant source of noise, and the other noise processes present in the system are assumed to be negligible.

3. The receiver is assumed to be employing a correlator followed by a decision device for the detection of received signals. If the input to this decision device is greater than or equal to a predetermined threshold, then a data bit "1" is declared to have been received. When the input to this decision device is lower than the threshold, then a data bit "0" is declared to have been received. The correlator is matched to the desired code sequence. While designing the OOCs, it is desirable that crosscorrelation between any two codewords is small.

4. Let an OOC $(n, w, \lambda_a, \lambda_c)$ has M codewords $C_1, C_2, \ldots, C_M$. Without loss of generality, we can assume one of the codewords as the desired codeword, and all other codewords as interfering codewords for the correlator. Since the maximum value of peak autocorrelation is w, for the transmission of a data bit "1", the output of the correlator is w when no other user is transmitting a data bit "1" in the same bit interval. Therefore, by setting the threshold at a value equal to w, no error is made while declaring it as a "1" at the receiver. If some users are transmitting a "1" simultaneously in the same bit interval, the output of correlator may exceed w. However, the decision device will declare it as a "1" only.

If a data bit "0" is transmitted, then the output of the correlator will be zero ideally when no other user is sending a data bit "1" in the same bit interval. The receiver can declare it to be a data bit "0" and make no error in the decision since the threshold is set at w. But, when a data bit "0" is transmitted, and some other users simultaneously transmit "1", then the output of the correlator may exceed w, thus forcing the decision device to declare a "1", and making an error.

5. We consider the case of the desired user sending a data bit "0" in the bit interval under consideration.

The maximum value of crosscorrelation gives the worst case scenario. In general, the value of crosscorrelation between any two codewords may not be equal to λ_c for every pair of codewords. The chip synchronism is assumed between different users at the correlator. This also gives us the worst case scenario. So any system designed for these constraints, will always give a better performance in real life.

The comparison of different OOCs in this section, is general in nature. A specific comparison may be done by computing bit error rates for lower values of thresholds. These are meaningful for similar values of parameters of different OOCs. For this, the individual interference patterns of the OOCs have to be used. The new OOCs proposed in this work have smaller weights, so a specific comparison by lowering the threshold may not be meaningful.

The maximum number of simultaneous users can be decided by specifying the tolerable limit for degradation in performance, as a result of multiple access interference. This number must also take into account the fact that only those users contribute to the multiple user interference, who transmit a data bit 1 in the same bit interval under consideration. The knowledge of the number of times the multiple user interference crosses the value of $(w-1)$ at the correlator output, will be helpful in practice. Other noise sources may cause the correlator output to exceed w under such situations, causing a "0" being falsely detected as a "1".

All these assumptions also hold for other OOCs discussed in this thesis. All the plots indicate the multiple user intereference, when the data bit corresponding to the desired user at the correlator input is "0", and all other users present have a data bit "1" in the bit interval under consideration. The area under the plots reflect the strength of the interference. The delays between the arrival of sequences corresponding to different users are random, given by an integer i, where $0 \leq i < n$ for a code length n.

Fig. 6.2.1 shows the output of the correlator, when three codewords of a $(25, 5, 4, 2)$ Prime Sequence OOC are present as interferers. The Prime Sequence codes have a maximum value of crosscorrelation of 2. When the number of users is increased by one, the interference pattern changes significantly, as shown in Fig. 6.2.2. Though no error can still occur, the interference pattern gets stronger around the value $(w - 1)$.

Let us now compare it with the OOC based on Quadratic Congruences. In Fig. 6.2.3, we show two interfering users, while in Fig. 6.2.4, the number of interfering users is 3. If we compare Fig. 6.2.1 with Fig. 6.2.4, we observe that the interference pattern (and also the areas under them) are quite similar. Difference, however, is that for similar code lengths and weights, the number of interfering users is one less for the Quadratic Congruence code. This can be attributed to the maximum crosscorrelation value of 4 in the case of OOCs based on Quadratic Congruences, compared to a value of 2 in the Prime Sequences codes.

The $(31, 7, 3, 3)$ Projective Geometry code has an increased length and larger correlation parameters to achieve the same number of codewords (4), as that of the Quadratic Congruence code. Fig. 6.2.6 shows that the interference pattern is stronger compared to that in Fig. 6.2.4, though λ_c is more in the case of codewords used in Fig. 6.2.4. This is due to the larger weights of codewords used for the OOC based on Projective Geometry. The threshold is also set accordingly higher in Figs. 6.2.5 and Fig. 6.2.6, when the number of interfering users is 3 in both the cases. The same

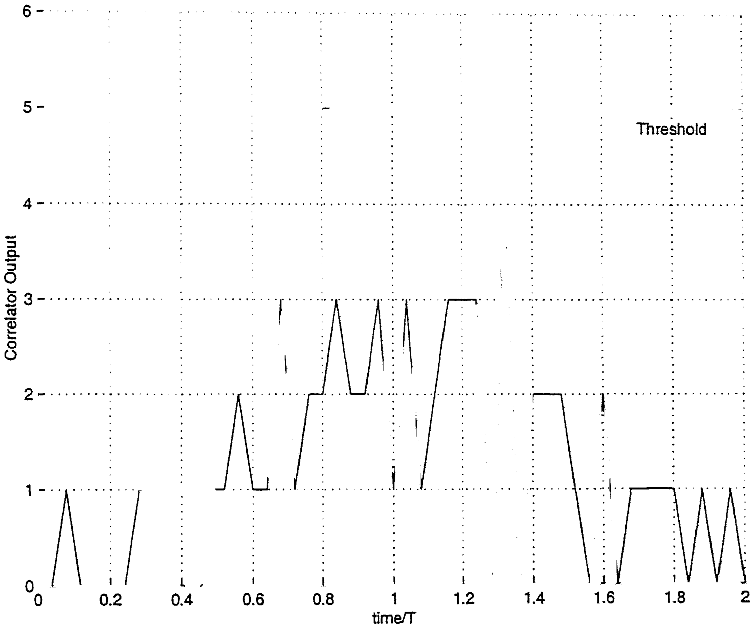

Figure 6.2.1: Output of the correlator matched to codeword C_3, when sequences corresponding to codewords C_1, C_2, and C_4, are present simultaneously at the input for a $(25, 5, 4, 2)$ OOC based on Prime Sequences

analogy holds for Figs. 6.2.3 and 6.2.5, where there are two interfering users.

The length of codewords is even smaller for $(15, 7, 3, 4)$ OOC using Hadamard matrices. The maximum crosscorrelation value is equal to 4, which is the same as in Quadratic Congruence codes. Comparing Fig. 6.2.7 with Fig. 6.2.4, with three interfering users in each case, we see that the interference is much stronger in Fig. 6.2.7. This is due to the increased weight. Therefore, reducing code lengths while increasing code weights to get more codewords is a poorer solution. Same can be said about Fig. 6.2.9. In fact, when four interfering users are present simultaneously, as in Figs. 6.2.8 and 6.2.10, with each interfering user transmitting a data bit "1" in the bit interval when the desired user sends a "0", then with a probability 1, this bit will be erroneously decoded.

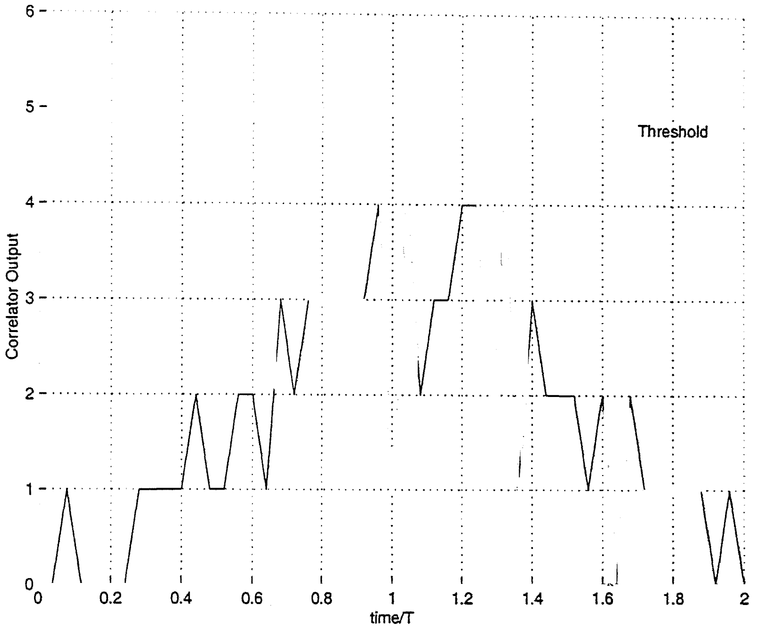

Figure 6.2.2: Output of the correlator matched to codeword C_3, when sequences corresponding to codewords C_1, C_2, C_4, and C_5, are present simultaneously at the input for a $(25, 5, 4, 2)$ OOC based on Prime Sequences

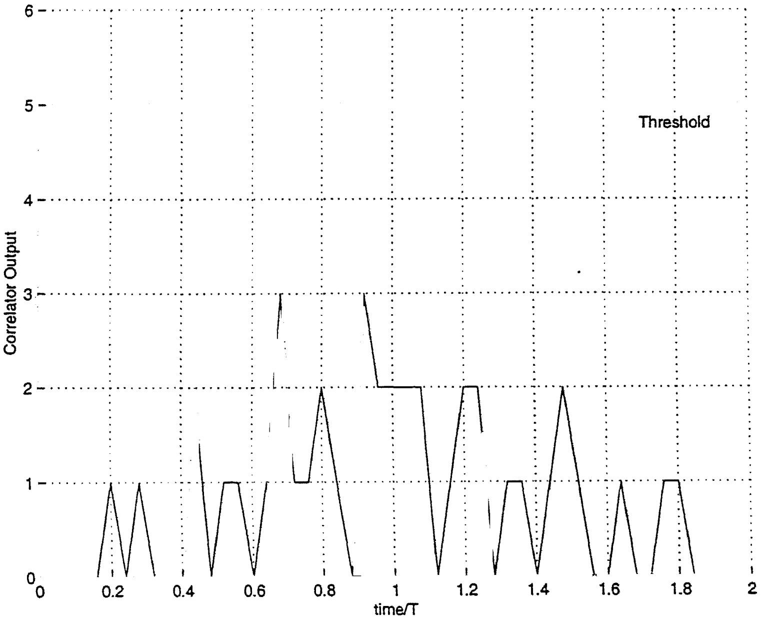

Figure 6.2.3: Output of the correlator matched to codeword C_3, when sequences corresponding to codewords C_1, and C_4, are present simultaneously at the input for a $(25, 5, 2, 4)$ OOC based on Quadratic Congruences

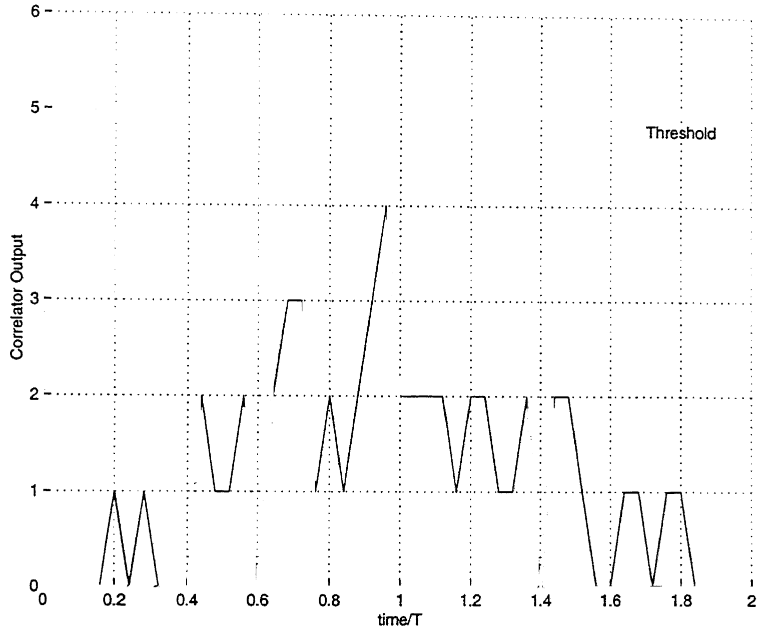

Figure 6.2.4: Output of the correlator matched to codeword C_3, when sequences corresponding to codewords C_1, C_2, and C_4, are present simultaneously at the input for a $(25, 5, 2, 4)$ OOC based on Quadratic Congruences

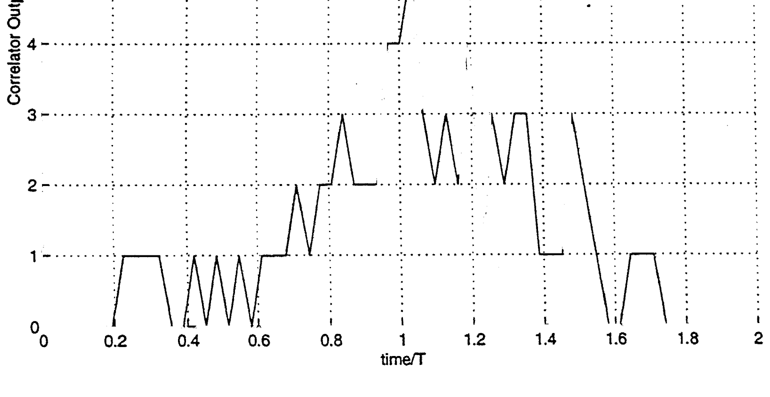

Figure 6.2.5: Output of the correlator matched to codeword C_3, when sequences corresponding to codewords C_1, and C_4, are present simultaneously at the input for a $(31, 7, 3, 3)$ OOC based on Projective Geometry

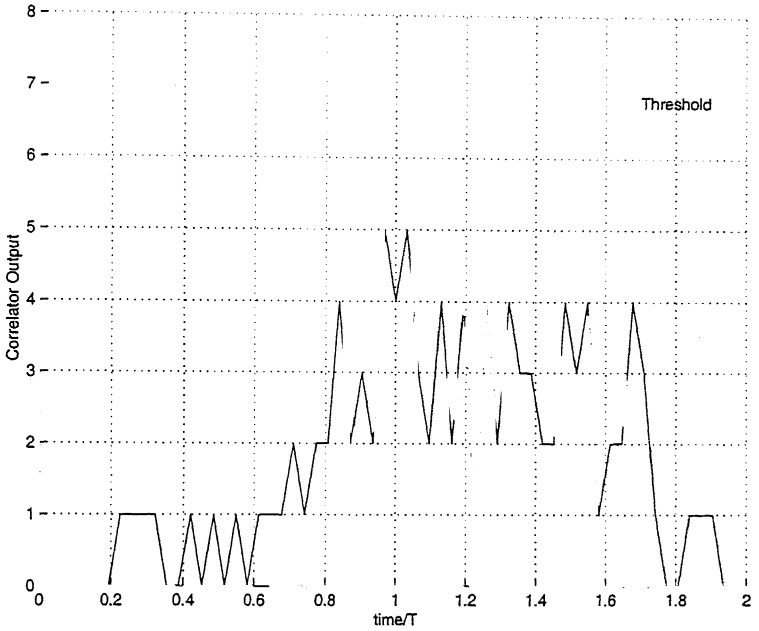

Figure 6.2.6: Output of the correlator matched to codeword C_3, when sequences corresponding to codewords C_1, C_2, and C_4, are present simultaneously at the input for a $(31, 7, 3, 3)$ OOC based on Projective Geometry

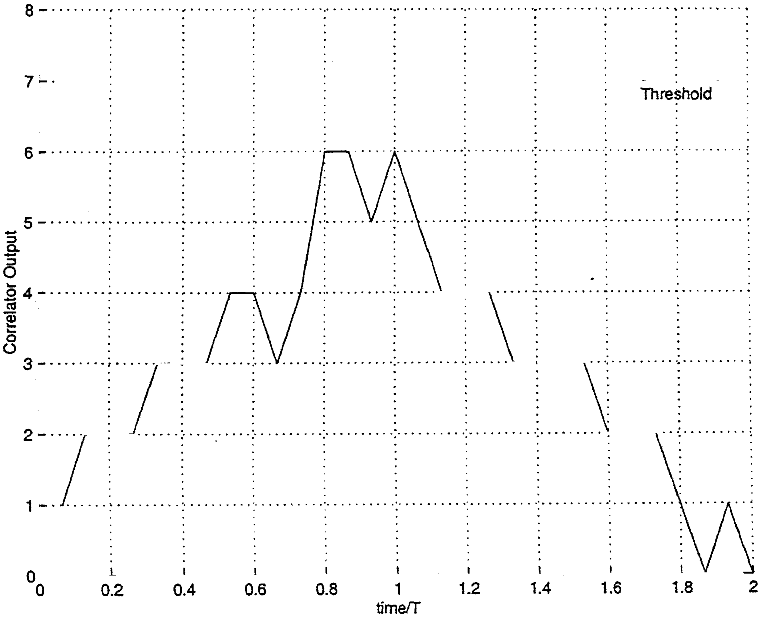

Figure 6.2.7: Output of the correlator matched to codeword C_7, when sequences corresponding to codewords C_2, C_3, and C_4, are present simultaneously at the input for a $(15, 7, 3, 4)$ OOC based on Hadamard matrices

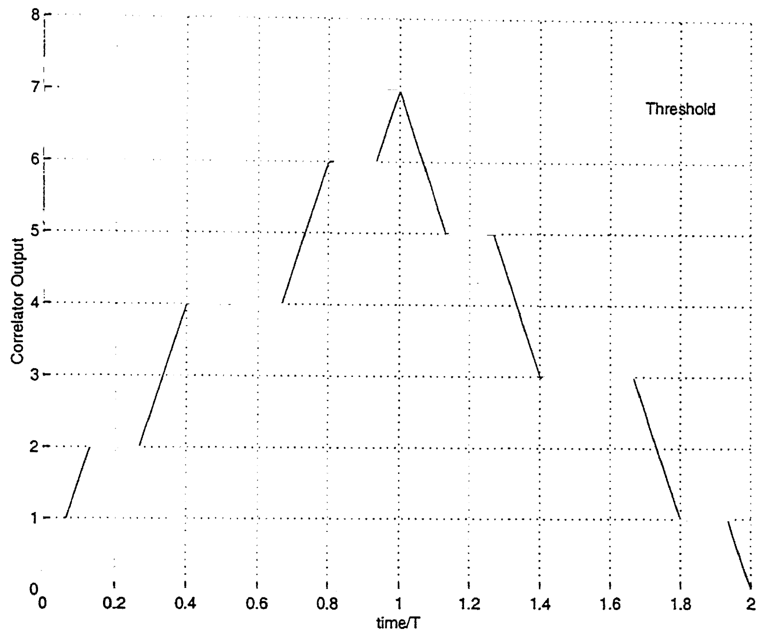

Figure 6.2.8: Output of the correlator matched to codeword C_7, when sequences corresponding to codewords C_2, C_3, C_4, and C_5, are present simultaneously at the input for a $(15,7,3,4)$ OOC based on Hadamard matrices

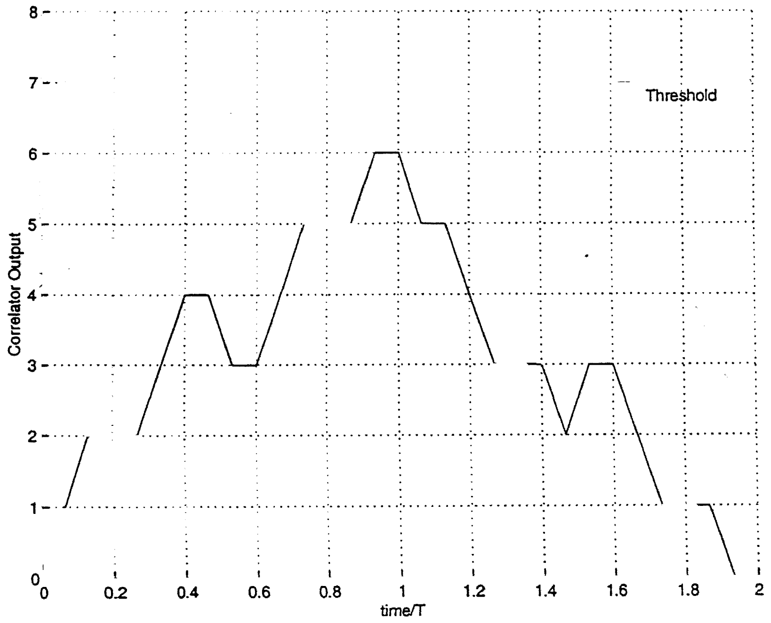

Figure 6.2.9: Output of the correlator matched to codeword C_7, when sequences corresponding to codewords C_8, C_9, and C_{10}, are present simultaneously at the input for a $(15,7,3,4)$ OOC based on Hadamard matrices

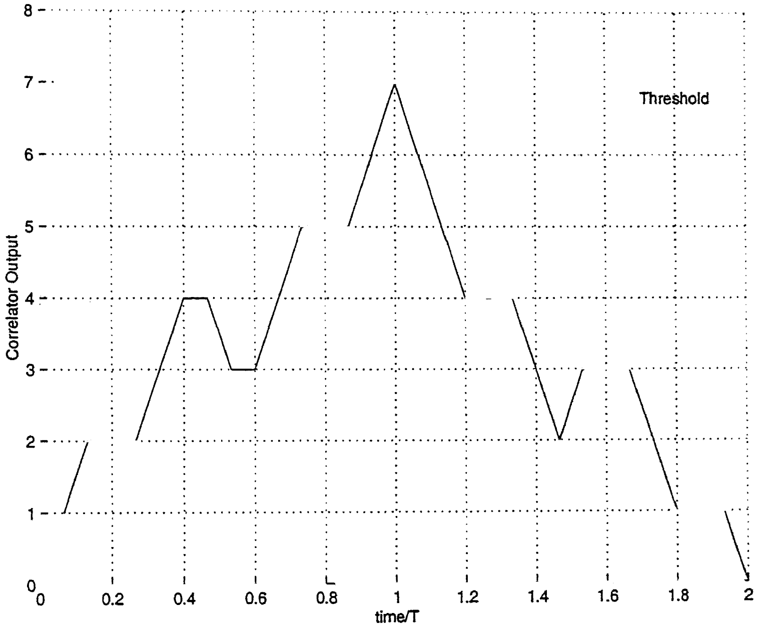

Figure 6.2.10: Output of the correlator matched to codeword C_7, when sequences corresponding to codewords C_8, C_9, C_{10}, and C_{11}, are present simultaneously at the input for a $(15, 7, 3, 4)$ OOC based on Hadamard matrices

The OOCs based on Skolem Sequences have the minimum possible length of codewords for the given code parameters. As seen in Figs. 6.2.1, 6.2.4, and 6.2.11, the interference patterns of OOCs based on Skolem sequences are the weakest compared to those of the Prime Sequence codes and the Quadratic Congruence codes. In all these cases, the code length is 25, and number of simultaneous users 3. This is due to the small value of $\lambda_c = 1$ for OOCs based on Skolem Sequences. Figs. 6.2.12 and 6.2.6 can be similarly compared for a code length equal to 31. The OOCs using Skolem Sequences are much better because they use the same length of codewords as that of $(31, 7, 3, 3)$ OOC using Projective Geometry, but, generate codewords having smaller crosscorrelations. The number of codewords is also increased by 1 in this case.

Figs. 6.2.1, 6.2.2, 6.2.13, and 6.2.14 show that though the crosscorrelation value $\lambda_c = 2$ is same for both the Prime Sequence codes and the OOCs obtained using the Number Theory approach, the performance of $(17, 3, 2, 2)$ code is poorer. This may be due to its lower weight, and consequently, a lower value of threshold.

The OOCs using the Table of Primes are variants of the Prime Sequence codes, and they trade crosscorrelation for better off-peak autocorrelation values. Therefore, Fig. 6.2.15 and 6.2.1 show that the Prime Sequence codes are better.

The OOCs using Quadratic Residues have a smaller λ_c as compared to Quadratic Congruence codes. Therefore, their performance is expected to be better. Figs. 6.2.6 and 6.2.16, however, do not substantiate this. This may be due to the fact that λ_c is the maximum crosscorrelation value which represents the worst case scenario that may not always happen.

We see that the OOCs using the Skolem Sequences, as proposed and discussed in Chapter 4, are not only optimal, but they also appear to have the best multiple access interference rejection capability, because of their crosscorrelation parameters. The value of λ_c in this case, is the minimum possible value of 1. The length of the codewords is also the minimum length theoretically possible.

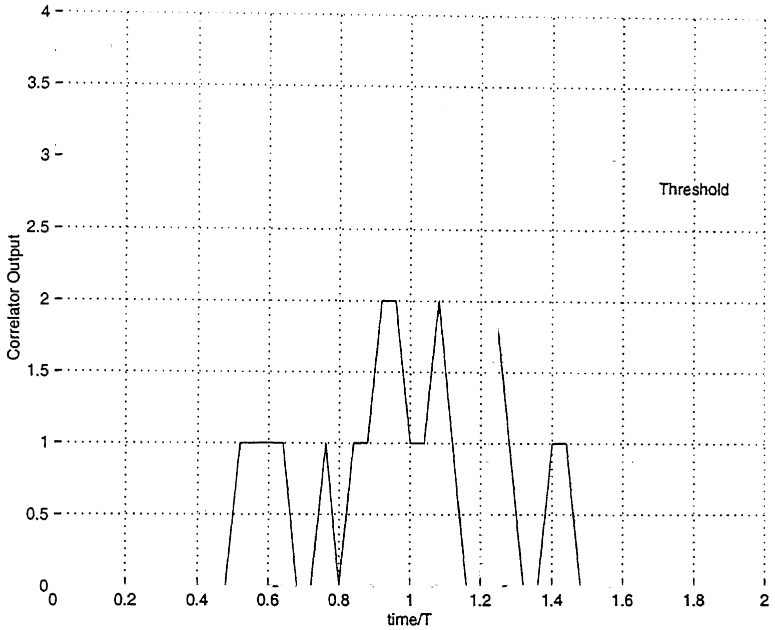

Figure 6.2.11: Output of the correlator matched to codeword C_4, when sequences corresponding to codewords C_1, C_2, and C_3, are present simultaneously at the input for a $(25, 3, 1, 1)$ OOC based on Skolem Sequences

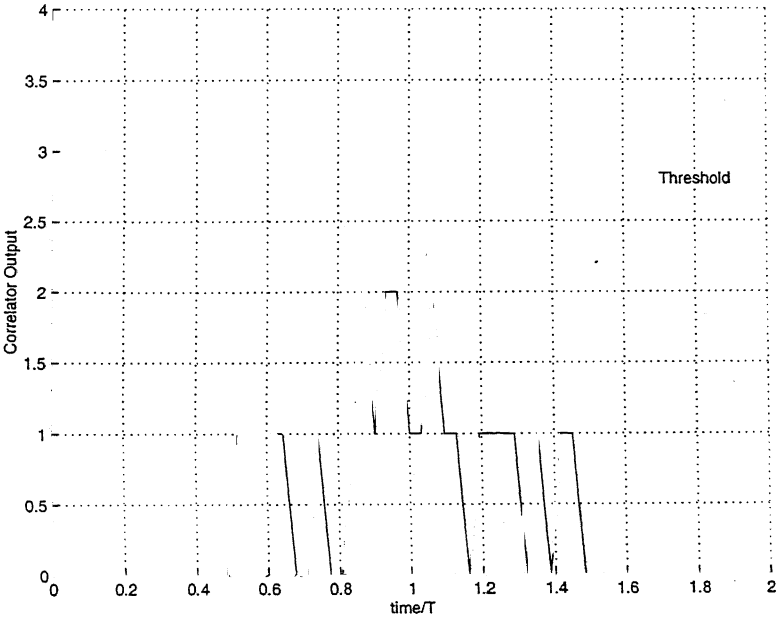

Figure 6.2.12: Output of the correlator matched to codeword C_5, when sequences corresponding to codewords C_1, C_2, C_3, and C_4, are present simultaneously at the input for a $(31, 3, 1, 1)$ OOC based on Skolem Sequences

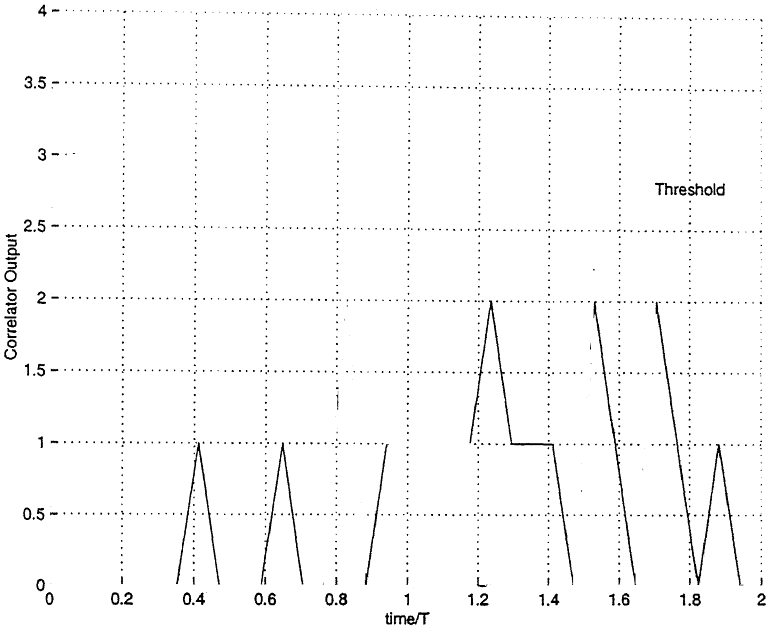

Figure 6.2.13: Output of the correlator matched to codeword C_5, when sequences corresponding to codewords C_1, C_2, and C_3, are present simultaneously at the input for a $(17, 3, 2, 2)$ OOC based on Number Theory

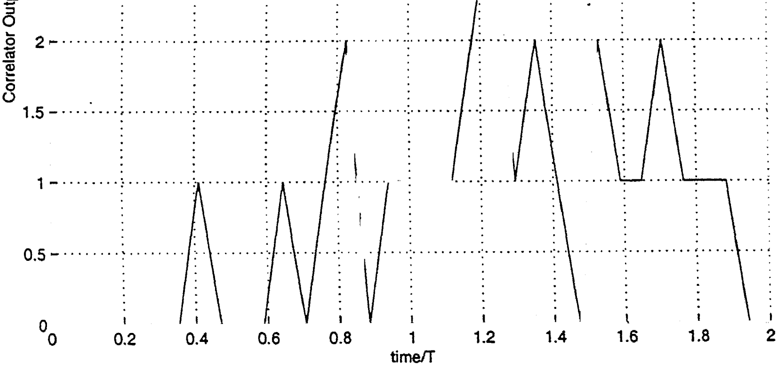

Figure 6.2.14: Output of the correlator matched to codeword C_5, when sequences corresponding to codewords C_1, C_2, C_3, and C_4, are present simultaneously at the input for a $(17, 3, 2, 2)$ OOC based on Number Theory

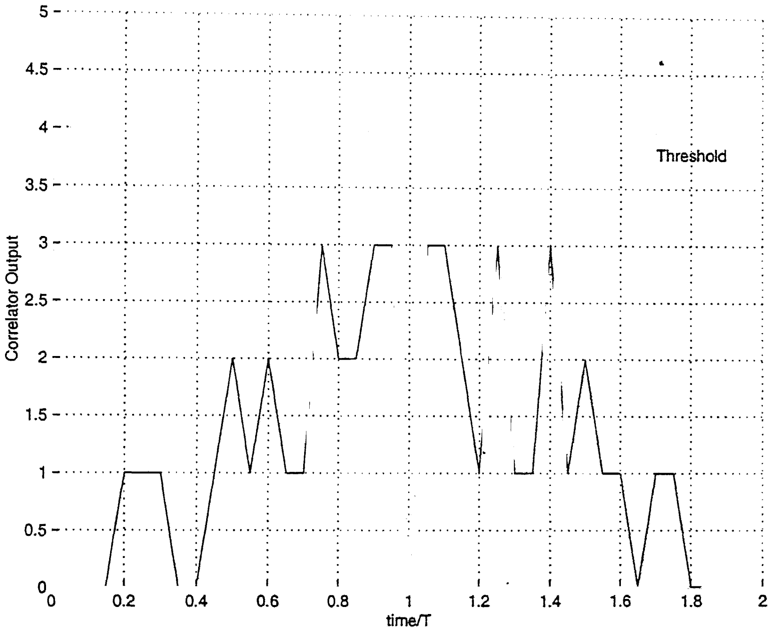

Figure 6.2.15: Output of the correlator matched to codeword C_4, when sequences corresponding to codewords C_1, C_2, and C_3, are present simultaneously at the input for a $(20, 4, 1, 3)$ OOC based on the Table of Primes

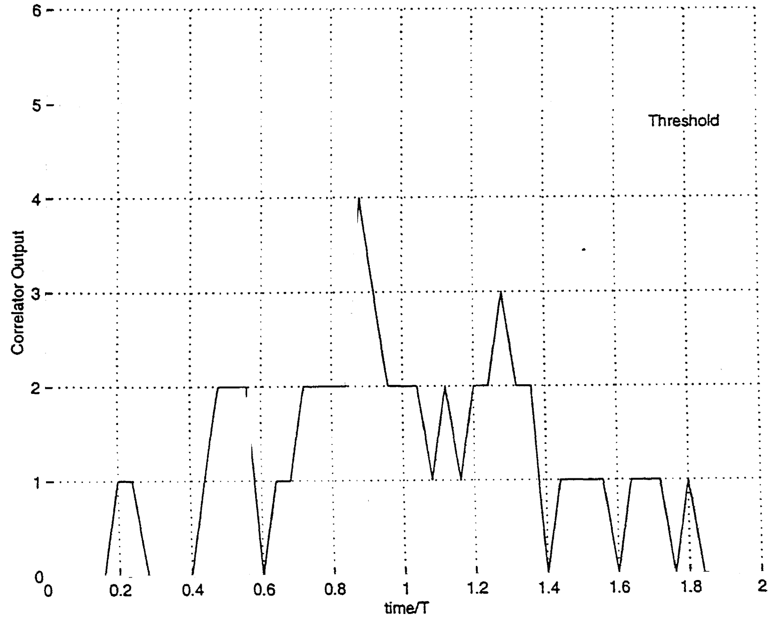

Figure 6.2.16: Output of the correlator matched to codeword C_4, when sequences corresponding to codewords C_1, C_2, and C_3, are present simultaneously at the input for a $(25, 5, 2, 2)$ OOC based on Quadratic Residues

Chapter 7

Conclusion

With the all optical networks becoming a reality, and immense advantages of CDMA in asynchronous multiple user environments, the use of CDMA in fiber optic local area networks has been proposed. The requirement to have a large number of simultaneous users having minimally interfering (0,1) code sequences has led to various classes of Optical Orthogonal Codes being suggested in the last two decades. The longer code lengths required to generate even a moderate number of codewords having desirable correlation properties, limit the data rates that can be supported. The focus of investigations in this work has been the construction of OOCs that have comparatively smaller code lengths and better crosscorrelation parameters. The following points summarize the work of this thesis and also suggest future work in this direction.

- A review of the Optical Orthogonal Codes, suggested earlier in the literature, has been carried out. We generalized the OOCs based on Projective Geometry and gave an illustrative example to construct codewords for $\lambda \geq 1$.

- We suggested a simpler method to generate codewords of Temporal/Spatial Codes for $\lambda_a = 0$. This construction directly uses the well known Prime Sequences to generate the codewords.

- A new class of OOCs is proposed, which is based on Hadamard matrices. The codewords generated using this method have smaller lengths, and can be generated for any code length n, if a Hadamard matrix exists for the corresponding order $(n+1)$. We included two illustrative examples to describe the construction procedure, before listing a generalized construction procedure.

- Skolem sequences of an order M consists of M pairs of integers from the set $\{1, 2, \ldots, 2M\}$, such that the elements of the pairs have distinct distances which form the set $\{1, 2, \ldots, M\}$. We suggested a translated version of these Skolem sequences to distinctly put integers in the distance sets of weight 3. We proposed a new class of OOCs using this method.

- Then, we proposed a new class of OOCs, using the Table of Primes. These codes are a variant of the Prime Sequence codes. Next, we used the Number Theory approach, and by partitioning $GF(n)$ into t 3-sets, we obtained another new class of OOCs with correlation constraints limited to 2.

- Another new class of OOCs using Quadratic Residues has been suggested. The codewords of this code appear similar, but, are distinct from the OOCs using Quadratic Congruences suggested earlier in the literature. This class has a maximum value of crosscorrelation of 2 between any two codewords, whereas for the Quadratic Congruence codes, this value is 4. All the other code parameters are exactly the same.

- Finally, we presented a brief comparison of the OOCs proposed in this thesis, with the OOCs already suggested in the literature. The notion of optimality used in this thesis is related to the number of codewords in the OOC. The Johnson bound gives the theoretically maximum possible number of codewords for the given code parameters. We observe that the OOCs constructed using a prime number as their basis, such as, Prime Sequences, Quadratic Congruences, etc., are not optimal. The OOCs using Hadamard matrices have a large number of codewords for given code parameters.

- The OOCs using Skolem Sequences are optimal codes for any code parameters. The codewords generated using this method have the minimum possible length. The codewords in this class of OOCs can be generated for any M, where M is the number of codewords, when M is either 0 (mod 4) or 1 (mod 4).

- The OOCs suggested in the thesis, particularly those based on Skolem Sequences, have good multiple access interference rejection capability. As the codewords in the suggested OOC have a lower weight, the computation of BER by lowering the threshold may not have been quite meaningful. The knowledge of the number of times the multiple access interference crosses the value of $(w - 1)$ at the correlator output may be helpful in practice, as any other additive noise source may cause a crossing of the threshold w, thus resulting in a detection error.

- A possible future direction of work, is to generalize the construction of OOCs using Skolem Sequences for weights greater than 3.

This thesis thus incorporates discussions on several new classes of OOCs, which have smaller code lengths and lower correlation constraints.

References

[1] A. A. Sawchuk and T. C. Strand, "Digital optical computing," *Proc. IEEE*, vol. 72, pp. 758–779, July 1984.

[2] R. Ramaswami and K. N. Sivarajan, *Optical Networks : A Practical Perspective.* San Francisco, California: Morgan Kauffmann, 1998.

[3] J. A. Salehi, "Emerging optical code-division multiple access communication systems," *IEEE Network*, pp. 31–39, March 1989.

[4] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks - part i : Fundamental principles," *IEEE Trans. on Communications*, vol. 37, pp. 824–833, August 1989.

[5] J. A. Salehi and C. A. Brackett, "Code division multiple-access techniques in optical fiber networks - part ii : Systems performance analysis," *IEEE Trans. on Communications*, vol. 37, pp. 834–842, August 1989.

[6] G. J. Foschini and G. Vannucci, "Using spread-spectrum in a high-capacity fiber-optic local network," *Journal of Lightwave Technology*, vol. 6, pp. 370–379, March 1988.

[7] G. Vannucci, "Combining frequency-division and code-division multiplexing in a high capacity optical network," *IEEE Network*, pp. 21–30, March 1989.

[8] G. Vannucci and S. Yang, "Experimental spreading and despreading of the optical spectrum," *IEEE Trans. on Communications*, vol. 37, pp. 777–780, July 1989.

[9] G. J. Pendock, M. J. L. Cahill, and D. D. Sampson, "Multi-gigabit per second demonstration of photonic code-division multiplexing," *Electronic Letters*, vol. 31, pp. 819–820, May 1995.

[10] K. P. Jackson, S. A. Newton, B. Moslehi, M. Tur, C. C. Cutler, J. W. Goodman, and H. J. Shaw, "Optical fiber delay-line signal processing," *IEEE Trans. Microwave Theory and Techniques*, vol. MTT-33, pp. 193–210, March 1985.

[11] A. A. Hassan, J. E. Hershey, and N. A. Riza, "Spatial optical cdma," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 609–613, April 1995.

[12] J. A. Salehi and E. Park, "Holographic cdma," *IEEE Trans. on Communications*, vol. 43, pp. 2434–2438, September 1995.

[13] M. E. Marhic, "Coherent optical cdma networks," *Journal of Lightwave Technology*, vol. 11, pp. 854–863, May-June 1993.

[14] W. Huang and I. Andonovic, "Coherent optical pulse cdma systems based on coherent correlation detection," *IEEE Trans. on Communications*, vol. 47, pp. 261–271, February 1999.

[15] J. A. Salehi, A. M. Weiner, and J. P. Heritage, "Coherent ultrashort light pulse code-division multiple access communication systems," *Journal of Lightwave Technology*, vol. 8, pp. 478–491, March 1990.

[16] D. J. Hajela and J. A. Salehi, "Limits to the encoding and bounds on the performance of coherent ultrashort light pulse code-division multiple-access systems," *IEEE Trans. on Communications*, vol. 40, pp. 325–336, February 1992.

[17] H. Fathallah, L. A. Rusch, and S. LaRochelle, "Optical frequency-hop multiple access communications system," in *Proc. of the International Conference on Communications (ICC)*, pp. 1269–1273, 1998.

[18] H. Fathallah, L. A. Rusch, and S. LaRochelle, "Passive optical fast frequency-hop cdma communications system," *Journal of Lightwave Technology*, vol. 17, pp. 397–405, March 1999.

[19] M. Kavehrad and D. Zaccarin, "Optical code-dvision-multiplexed systems based on spectral encoding of noncoherent sources," *Journal of Lightwave Technology*, vol. 13, pp. 534–545, March 1995.

[20] I. Hinkov, V. Hinkov, K. Iversen, and O. Ziemann, "Feasibility of optical cdma using spectral encoding by acoustically tunable optical filters," *Electronic Letters*, vol. 31, pp. 384–385, March 1995.

[21] E. D. J. Smith, P. T. Gough, and D. P. Taylor, "Noise limits of optical spectral-encoding cdma systems," *Electronic Letters*, vol. 31, pp. 1469–1470, August 1995.

[22] S. V. Marić, O. Moreno, and C. J. Corrada, "Multimedia transmission in fiber-optic lans using optical cdma," *Journal of Lightwave Technology*, vol. 14, pp. 2149–2153, October 1996.

[23] R. M. Gagliardi, A. J. Mendez, M. R. Dale, and E. Park, "Fiber-optic digital video multiplexing using optical cdma," *Journal of Lightwave Technology*, vol. 11, pp. 20–26, January 1993.

[24] E. Marom, "Optical delay line matched filters," *IEEE Trans. Circuits Systems*, vol. CAS-25, pp. 360–364, June 1978.

[25] Y. L. Chang and M. E. Marhic, "Fiber-optic ladder networks for inverse decoding coherent cdma," *Journal of Lightwave Technology*, vol. 10, pp. 1952–1962, December 1992.

[26] B. Moslehi, J. W. Goodman, M. Tur, and H. J. Shaw, "Fiber optic lattice signal processing," *Proc. IEEE*, vol. 72, pp. 909–930, July 1984.

[27] W. C. Kwong and P. R. Pruncal, "All-serial coding architecture for ultrafast optical code-division multiple-access," in *Proc. of the International Conference on Communications (ICC)*, pp. 552–556, 1993.

[28] J. G. Zhang, "Novel tunable ultra-high-speed optical fiber code-division multiple-access networks for real-time computer communications," in *Proc. of the International Conference on Communications (ICC)*, pp. 1322–1326, 1995.

[29] W. C. Kwong, G. C. Yang, and J. G. Zhang, "2^n prime-sequence codes and their optical cdma coding architecture," in *Proc. of the International Conference on Communications (ICC)*, pp. 1317–1321, 1995.

[30] T. Ohtsuki, I. Sasase, and S. Mori, "Effects of hard-limiter and error correction coding on performance of direct-detection optical cdma systems with ppm signaling," in *Proc. of the International Conference on Communications (ICC)*, pp. 1307–1311, 1995.

[31] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam: North-Holland, 1977.

[32] F. R. K. Chung, J. A. Salehi, and V. K. Kei, "Optical orthogonal codes : Design, analysis and applications," *IEEE Trans. Information Theory*, vol. 35, pp. 595–604, May 1989.

[33] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, May 1980.

[34] S. Tamura, S. Nakano, and K. Okazaki, "Optical code-multiplex transmission by gold sequences," *Journal of Lightwave Technology*, vol. LT-3, pp. 121–127, February 1985.

[35] C. Argon and R. Ergül, "Optical cdma via shortened optical orthogonal codes based on extended sets," *Optics Communications*, vol. 116, pp. 326–330, May 1995.

[36] A. A. Shaar and P. A. Davis, "Prime sequences : Quasi-optimal sequences for or channel code division multiplexing," *Electronic Letters*, vol. 19, pp. 888–889, October 1983.

[37] A. S. Holmes and R. R. A. Syms, "All-optical cdma using "quasi-prime" codes," *Journal of Lightwave Technology*, vol. 10, pp. 279–286, February 1992.

[38] E. Park, A. J. Mendez, and E. M. Garmire, "Temporal/spatial optical cdma networks - design, demonstration, and comparison with temporal networks," *IEEE Photonics Technology Letters*, vol. 4, pp. 1160–1162, October 1992.

[39] S. V. Marić, Z. I. Kostić, and E. L. Titlebaum, "A new family of optical code sequences for use in spread-spectrum fiber-optic local area networks," *IEEE Trans. on Communications*, vol. 41, pp. 1217–1221, August 1993.

[40] W. C. Kwong and G. C. Yang, "Construction of 2^n prime-sequence codes for optical code division multiple access," *IEE Proc. on Communications*, vol. 142, pp. 141–150, June 1995.

[41] W. C. Kwong, G. C. Yang, and J. C. Zhang, "2^n prime-sequence codes and coding architecture for optical code-division multiple-access," *IEEE Trans. on Communications*, vol. 44, pp. 1152–1162, September 1996.

[42] P. R. Pruncal, M. A. Santoro, and T. R. Fan, "Spread spectrum fiber-optic local area network using optical processing," *Journal of Lightwave Technology*, vol. LT-4, pp. 547–554, May 1986.

[43] P. R. Prucnal, M. A. Santoro, and S. K. Sehgal, "Ultrafast all-optical synchronous multiple access fiber networks," *IEEE Journal on Selected Areas in Communications*, vol. SAC-4, pp. 1484–1493, December 1986.

[44] G. C. Yang and W. C. Kwong, "Performance analysis of optical cdma with prime codes," *Electronic Letters*, vol. 31, pp. 569–570, March 1995.

[45] K. Sato, T. Ohtsuki, H. Uehara, and I. Sasase, "Performance of optical direct-detection cdma systems using prime sequence codes," in *Proc. of the International Conference on Communications (ICC)*, pp. 1312–1316, 1995.

[46] S. V. Marić, "New family of algebraically designed optical orthogonal codes for use in cdma fiber-optic networks," *Electronic Letters*, vol. 29, pp. 538–539, March 1993.

[47] Z. Kostić and E. L. Titlebaum, "The design and performance analysis for several new classes of codes for optical synchronous cdma and for arbitrary-medium time-hopping synchronous cdma communication system," *IEEE Trans. on Communications*, vol. 42, pp. 2608–2617, August 1994.

[48] W. C. Kwong, P. A. Perrier, and P. R. Pruncal, "Performance comparison of asynchronous and synchronous code-division multiple-access techniques for fiber-optic local area networks," *IEEE Trans. on Communications*, vol. 39, pp. 1625–1634, November 1991.

[49] C. Argon and H. F. Ahmad, "Optimal optical orthogonal code design using difference sets and projective geometry," *Optics Communications*, vol. 118, pp. 505–508, August 1995.

[50] M. Choudhary, P. K. Chatterjee, and J. John, "Code sequences for fiber optic cdma systems," in *Proc. of National Conference on Communications 1995, IIT Kanpur*, pp. 35–42, 1995.

[51] E. S. Shivaleela, K. N. Sivarajan, and A. Selvarajan, "Temporal/spatial codes for asynchronous fiber optic cdma network: Design and performance," in *Proc. of National Conference on Communications 1996, IIT Bombay*, pp. 23–26, 1996.

[52] E. S. Shivaleela, K. N. Sivarajan, and A. Selvarajan, "Design of a new family of two-dimensional codes for fiber-optic cdma networks," *Journal of Lightwave Technology*, vol. 16, pp. 501–508, April 1998.

[53] K. Kitayama, "Novel spatial spread spectrum based fiber optic cdma networks for image transmission," *IEEE Journal on Selected Areas in Communications*, vol. 12, pp. 762–772, May 1994.

[54] G. C. Yang and K. C. Kwong, "Two-dimensional spatial codes for image transmission in multicore-fibre cdma networks," *Electronic Letters*, vol. 31, pp. 1482–1483, August 1995.

[55] G. C. Yang and W. C. Kwong, "Two-dimensional spatial signature patterns," *IEEE Trans. on Communications*, vol. 44, pp. 184–191, February 1996.

[56] K. Kitayama, M. Nakamura, Y. Igasaki, and K. Kaneda, "Image fiber-optic two-dimensional parallel links based upon optical space-cdma : Experiment," *Journal of Lightwave Technology*, vol. 15, pp. 202–212, February 1997.

[57] S. Kim, K. Yu, and N. Park, "A new family of space/wavelength/time spread three-dimensional optical code for oocdma networks," *Journal of Lightwave Technology*, vol. 18, pp. 502–511, April 2000.

[58] L. Tančevski and I. Andonovic, "Block multiplexing codes for incoherent asynchronous all-optical cdma using ladder network correlators," *IEE Proc. on Optoelectronics*, vol. 142, pp. 125–131, June 1995.

[59] H. Chung and P. V. Kumar, "Optical orthogonal codes - new bounds and an optimal construction," *IEEE Trans. Information Theory*, vol. 36, pp. 866–873, July 1990.

[60] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Information Theory*, vol. 36, pp. 1334–1380, November 1990.

[61] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Information Theory*, vol. 38, pp. 940–949, May 1992.

[62] S. Bitan and T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families," *IEEE Trans. Information Theory*, vol. 41, pp. 77–87, January 1995.

[63] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Information Theory*, vol. 41, pp. 448–455, March 1995.

[64] G. C. Yang, "Some new families of optical orthogonal codes for code-division multiple-access fibre-optic networks," *IEE Proc. on Communications*, vol. 14, pp. 363–368, December 1995.

[65] S. V. Marić, M. D. Hahm, and E. L. Titlebaum, "Construction and performance analysis of a new family of optical orthogonal codes with ideal auto- and cross-correlation functions for use in cdma fiber-optic lans," in *Proc. of the International Conference on Communications (ICC)*, pp. 136–139, 1994.

[66] G. C. Yang and T. E. Fuja, "Optical orthogonal codes with unequal auto- and cross-correlation constraints," *IEEE Trans. Information Theory*, vol. 41, pp. 96–106, January 1995.

[67] G. C. Yang, "Variable-weight optical orthogonal codes for cdma networks with multiple performance requirements," *IEEE Trans. on Communications*, vol. 44, pp. 47–55, January 1996.

[68] C. Zhi, F. Pingzhi, and J. Fan, "Disjoint difference sets, difference triangle sets, and related codes," *IEEE Trans. Information Theory*, vol. 38, pp. 518–522, March 1992.

[69] M. Choudhary, P. K. Chatterjee, and J. John, "Optical orthogonal codes using hadamard matrices," in *Proc. of National Conference on Communications 2001, IIT Kanpur*, pp. 209–211, 2001.

[70] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs.* CRC Press, 1996.

[71] M. Hall, *Combinatorial Theory.* John Wiley and Sons, 1986.

[72] A. V. Geramita and J. Seberry, *Orthogonal Designs : Quadratic Forms and Hadamard Matrices.* New York: Marcel Dekker, 1979.

[73] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, pp. 1715–1729, December 1976.

[74] K. B. Letaief, "The performance of optical fiber direct-sequence spread-spectrum multiple access communications systems," *IEEE Trans. on Communications*, vol. 43, pp. 2662–2666, November 1995.

[75] L. B. Nelson and H. V. Poor, "Performance of multiuser detection for optical cdma-part i: Error probabilities," *IEEE Trans. on Communications*, vol. 43, pp. 2803–2811, November 1995.

[76] L. B. Nelson and H. V. Poor, "Performance of multiuser detection for optical cdma-part ii: Asymptotic analysis," *IEEE Trans. on Communications*, vol. 43, pp. 3015–3024, December 1995.

[77] H. Walle and U. Killat, "Combinatorial ber analysis of synchronous optical cdma with prime sequences," *IEEE Trans. on Communications*, vol. 43, pp. 2894–2895, December 1995.

[78] A. W. Lam and A. M. Hussain, "Performance analysis of direct detection optical cdma communication systems with avalanche photodiodes," *IEEE Trans. on Communications*, vol. 40, pp. 810–820, April 1992.

[79] H. M. Kwon, "Optical orthogonal code-division multiple-access system - part i : Apd noise and thermal noise," *IEEE Trans. on Communications*, vol. 42, pp. 2470–2479, July 1994.

[80] H. M. Kwon, "Optical orthogonal code-division multiple-access system - part ii : Multibits/sequence-period oocdma," *IEEE Trans. on Communications*, vol. 42, pp. 2592–2599, August 1994.

[81] C. L. Ho and C. Y. Wu, "Performance analysis of cdma optical communication systems with avalanche photodiodes," *Journal of Lightwave Technology*, vol. 12, pp. 1062–1072, June 1994.

[82] E. L. Walker, "A theoretical analysis of the performance of code division multiple access communications over multimode optical fiber channels - part i : Transmission and detection," *IEEE Journal on Selected Areas in Communications*, vol. 12, pp. 751–761, May 1994.

[83] E. L. Walker, "A theoretical analysis of the performance of code division multiple access communications over multimode optical fiber channels - part ii : System performance evaluation," *IEEE Journal on Selected Areas in Communications*, vol. 12, pp. 976–983, June 1994.

[84] L. A. Rusch and H. V. Poor, "Effects of laser phase drift on coherent optical cdma," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 577–591, April 1995.

[85] R. F. Ormondroyd and M. M. Mustapha, "Optically orthogonal cdma system performance with optical amplifier and photodetector noise," *IEEE Photonics Technology Letters*, vol. 11, no. 5, pp. 617–619, 1999.

Appendix A

Difference Families

In this Appendix, we discuss briefly about difference families and difference sets [70, 71]. We also present brief tables for cyclic difference sets for a few values.

Definition A.0.1 A *Balanced Incomplete Block Design* (BIBD) is a pair (V,B) where V is a v-set and B is a collection of b k-subsets of V (blocks) such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. The numbers (v, b, r, k, λ) are *parameters* of the BIBD.

Trivial and necessary conditions for the existence of a $BIBD(v, b, r.k.\lambda)$ are (1) $vr = bk$, and (2) $r(k-1) = \lambda(v-1)$.

Definition A.0.2 Let G be an additive abelian group of order n. Then t w-element subsets of G, $B_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,w}\}$, $where\ \ 1 \leq i \leq t$, forms a (n, w, λ) *difference family* if every nonzero element of G occurs λ times as the differences $\{b_{i,x} - b_{i,y}\}, where\ \ \{i = 1, 2, \ldots, t;\ \ x, y = 1, 2, \ldots, w\}$.The sets B_i are called *base blocks*.

If $t = 1$, then B_i is an abelian difference set (n, w, λ). If $B_1, B_2, \ldots, B_t$ forms a (n, w, λ) difference family, then the translates of the base blocks, namely $B_i + g = \{b_{i,1} + g, b_{i,2} + g, \ldots, b_{i,w} + g\}$, $where\ \ \{i = 1, 2, \ldots, t,\ g \in G\}$, forms a (n, w, λ) *Balanced Incomplete Block Design* (BIBD).

Table A.1: Base Blocks of $(n,3,1)$ cyclic difference families

n	Base Blocks
7	(0,1,3)
13	(0,1,4) (0,2,7)
15	(0,1,4) (0,2,9)
19	(0,1,4) (0,2,9) (0,5,11)
21	(0,1,3) (0,4,12) (0,5,11)
25	(0,1,3) (0,4,11) (0,5,13) (0,6,15)
27	(0,1,3) (0,4,11) (0,5,15) (0,6,14)
31	(0,1,12) (0,2,24) (0,3,8) (0,4,17) (0,6,16)
33	(0,1,3) (0,4,10) (0,5,18) (0,7,19) (0,8,17)
37	(0,1,3) (0,4,26) (0,5,14) (0,6,25) (0,7,17) (0,8,21)
39	(0,1,3) (0,4,18) (0,5,27) (0,6,16) (0,7,15) (0,9,20)
43	(0,1,3) (0,4,9) (0,6,28) (0,7,23) (0,8,33) (0,11,30) (0,12,26)
45	(0,1,3) (0,4,10) (0,5,28) (0,7,34) (0,8,32) (0,9,29) (0,12,26)
49	(0,1,3) (0,4,9) (0,6,17) (0,7,23) (0,8,30) (0,10,31) (0,12,36) (0,14,34)
51	(0,1,3) (0,4,9) (0,6,25) (0,7,35) (0,8,22) (0,10,21) (0,12,27) (0,13,31)

Definition A.0.3 If $v = k(k-1)t + 1$, then t blocks $B_i = \{b_{i,1}, b_{i,2}, \dots, b_{i.k}\}$ form a *perfect* $(v, k, 1)$ difference family over $\mathbb{Z}_v$ if the $tk(k-1)/2$ differences $b_{i,m} - b_{i,n}$; $(i = 1, 2, \dots, t;\ \ 1 \leq m < n \leq k)$ cover the set $\{1, 2, \dots, (v-1)/2\}$.

Let G be an additively written group of order v. A k-subset D of G is a $(v, k, \lambda; n)$-difference set of order $n = k - \lambda$ if every nonzero element of G has exactly λ representations as a difference $d - d'$ with elements from D. The difference set is abelian, cyclic etc., if the group G has the respective property.

The tables A.1 - A.3 show different cyclic difference families for a few values.

Appendix B

Existence Conjectures for Hadamard Matrices

This Appendix presents the necessary conditions and existence conjectures for Hadamard matrices [70–72].

Theorem B.0.1 *If there is a Hadamard matrix H_n, then $n = 1, 2$ or $4k$, where k is a positive integer.*

Theorem B.0.2 *If there exists a Hadamard matrix $H_n = (h_{ij})$, and a Hadamard matrix $H_m = (l_{ij})$, then there is a Hadamard matrix $H_{mn} = (k_{ij})$, obtained by setting $k_{na+i,mb+j} = l_{ab}h_{ij}$ for $0 \leq a, b \leq m$ and $0 \leq i, j \leq n$.*

Theorem B.0.3 *If a Hadamard matrix H_n exists, then the Hadamard matrix $H_{2^t n}$ also exists for all $t > 0$.*

Appendix C

Existence and Construction of Skolem Sequences

In this Appendix, we briefly mention the existence conditions and construction techniques for Skolem sequences [70].

Theorem C.0.4 *A Skolem sequence of order n exists if and only if $n \equiv 0 \pmod{4}$ or $n \equiv 1 \pmod{4}$.*

Construction of Skolem Sequences : Skolem sequences can be constructed using the following procedure:

1. When $n = 1$, take $\{(1,2)\}$.
2. When $n = 4$, take $\{(1,2),\ (5,7),\ (3,6)\ (4,8)\}$.
3. When $n = 5$, take $\{(1,2),\ (7,9),\ (3,6)\ (4,8)\ (5,10)\}$.
4. For $n > 5$, use the following for construction of ordered pairs:

$$n = 4s : \begin{cases} (4s + r + 1, 8s - r + 1) & r = 1, \ldots, 2s \\ (r, 4s - r - 1) & r = 1, \ldots, s - 2 \\ (s + r + 1, 3s - r) & r = 1, \ldots, s - 2 \\ (s - 1, 3s),\ (s, s + 1),\ (2s, 4s - 1),\ (2s + 1, 6s) & \end{cases} \tag{C.1}$$

$$n = 4s+1: \begin{cases} (4s+r-1, 8s-r+3) & r = 1, \ldots, 2s \\ (r, 4s-r+1) & r = 1, \ldots, s \\ (s+r+2, 3s-r+1) & r = 1, \ldots, s-2 \\ (s+1, s+2),\ (2s+1, 6s+2),\ (2s+2, 4s+1) & \end{cases} \tag{C.2}$$

Appendix D

Table of Primes and Primitive Roots

In this Appendix, we present a brief table of Primes and their primitive roots [70].

Prime Number p	Primitive Root α
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2
31	3
37	2
41	6
43	3
47	5
53	2
59	2
61	2
67	2
71	7
73	5
79	3
83	2

Table D.1: Table of Primes p and Primitive Roots α